IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 12, Issue 4, Ver. IV (Jul.-Aug. 2017), PP 36-44
www.iosrjournals.org

A Novel Database Assited System for Smart Living Using Iot

*K.Sreeja[1], Mr. M. Sunil Babu[2]
[1] Project Student, Department of E.C.E, Vasireddy Venkatadri Institute of Technology, Nambur, AP,India
[2] Assoc. Professor, Department of E.C.E, Vasireddy Venkatadri Institute of Technology, Nambur, AP, India
Corresponding Author: K.Sreeja

Abstract: *In this advanced and rapid changing environment, smart living is taking different twists and turns in such of efficient systems that helps in every aspect of living. An advanced Internet of Things (IoT) refers to the possibility of connecting sensors, actuators or any device to the Internet. It can lead to a significant change in our daily lives in the way we live and interact with the devices such as home appliances, smart meters, security sensors, HVAC systems, etc. To apply IoT to the ambient assisted living platform, investigations need to be made at different levels. With IoT, data can be stored on cloud and can be accessed from anywhere. The system uses IEEE 802.11 WiFi standard as a communication link between devices and cloud. Data can be accessed and managed in a very cozy environment. The system uses WemosD1 R2 microcontroller with ESP8266 WiFi module built-in. We can use any free cloud service to store data or design a custom database to store the data.*

Keywords: *Internet of Things (IoT).*

Date of Submission: 03-08-2017 Date of acceptance: 17-08-2017

I. Introduction

Smart Home is the term commonly used to define a residence that uses a Home Controller to integrate the residence's various home automation systems. The most popular Home Controllers are those that are connected to a Windows based PC during programming only, and are then left to perform the home control duties on a standalone basis. Integrating the home systems allows them to communicate with one another through the home controller, thereby enabling single button and voice control of the various home systems simultaneously, in preprogrammed scenarios or operating modes.

Advancements in the field of smart homes are not an isolated case.

1. The developments take place within the society and are influenced by trends within that society.
2. In order to create added value the focus should be on the smart home environment instead of only on the used technology.
3. Creating smart environments to support elderly and disabled persons has enormous potential.

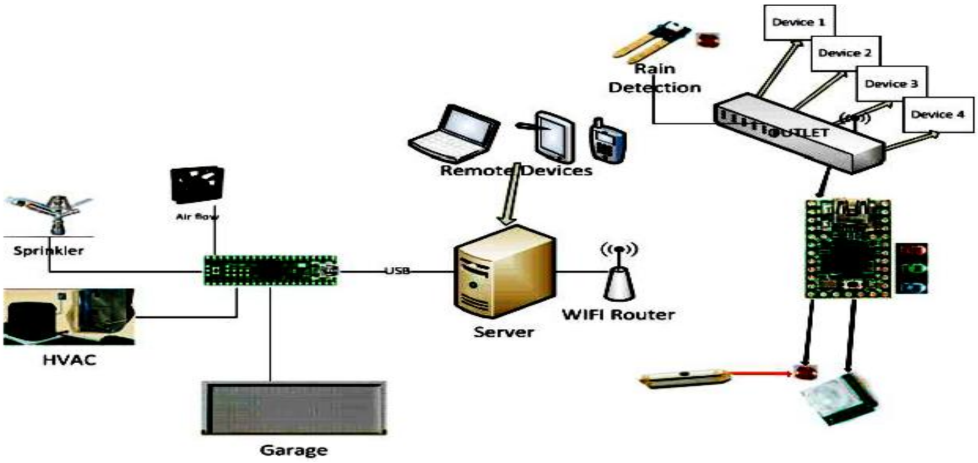

Fig .1 Smart Home Scenarios

Fig 1 shows the available scenarios in the smart home automation. It contains controllers, sensors and other communication modules to provide interaction between various components and controllers. We can even store data in the server which is located at a centralized area. The data from the server can be accessed from anywhere in the world.

II. Literature Survey

Various technologies were introduced earlier in the smart home technology. Extensive research took place in the recent part. Nowadays, the security level is very important, always emphasized and enhanced system. Different ways of security system have been enhanced such as use a large number of security officers, the use of sophisticated weapons, the use of alarms, monitoring system, through the production of electronic hardware and software and much more. All of this improvement depends on their usage. One of the most important safety system and required for all social group is home security. Houses need to be monitored at all times such as from theft, fire and short circuits. Recently, the rate of crimes involving robbery, murder and fires is increasing and worrying all of us.

These devices, along with the home database, have a variety of personal information regarding a home's inhabitants, like healthcare information, financial information, videos, pictures, live video feeds from home, daily habits or routines, favorite music, movies, and sometimes even a personal dairy. In some rare cases, inhabitants may use implanted medical devices, which need to be remotely accessed by hospitals or medical professionals, which can be done through the home network. Different devices used, bring different security vulnerabilities to the smart home, so, if or when these modern homes are compromised, they present a greater threat to the privacy and physical wellbeing of the home's inhabitants than ever before. A lot of research has gone into automating the home [10] [11], making it accessible via the Internet [12] or mobile phones [13] [14], saving energy [15], technology assisted living for senior citizens [16], and security [17]. Existing research only addresses and proposes defenses against normal intrusion attempts at home, and doesn't consider the risk of intrusion from sophisticated or tech-savvy criminals.

Our work mainly focuses on the security aspect of home automation. We first discuss how the concept of security has changed in modern home automation systems, then focus on various challenges in the field from a security point of view. The paper goes on to discuss various home automation systems and their security issues based on methodology used: context-aware home automation, central controller- based home automation, Bluetooth- based home automation, mobile or GSM- based home automation, Internet- based home automation, and a decentralized approach to home automation.

Commonly used technologies and networks for home automation have many vulnerabilities, as discussed by C. Karlof and D. Wagner [18]. They consider various routing attacks on wireless sensor networks (WSNs). This includes Sinkhole attacks, Selective Forwarding attacks, Sybil attacks, and Cloned ID attacks. In 2006, Y.C Hu et al. [19] detected an important attack on wireless networks called a Wormhole attack in which the attacker records data packets in the network at one location, tunnels them to another location, and retransmits them to the network. This attack can be carried out even if all communications in the network are done with confidentiality and integrity using IP sec in 6LoWPAN.

Data packet integrity, device authenticity, key establishment, and encryption standards are specified in almost all wireless encryption protocols these days. In 2011, J. Wright et al. [20] showed how a ZigBee or 802.15.4 wireless networks can be hacked using replay attacks [21]. During reflashing, the new key is sent in plain text over the air. An attacker can take advantage of this and sniff for encryption keys in plain text, inject, decode, and alter data packets to manipulate a device's operations. In 2013, B. Fouladi and S. Ghanoun [22] demonstrated a vulnerability in Z-Wave door locks, which gave the attacker full access without proper authorization. In 2013, T. Oluwafemi et al. [23] showed how a simple device in a home, such as a fluorescent lamp (CFL), which is connected to a home automation network or Internet could be manipulated to cause physical harm (shattered glass, fire outbreak, mercury poisoning) to a home's inhabitants. Moreover, lights fluctuating at certain frequencies could be very dangerous for people with photosensitive epilepsy [24].

When a home automation network is connected to the Internet, there is the possibility that an attacker could gain control of switches and dimmers along with devices plugged into the power outlets. Researchers also discussed the presence of some well-known vulnerabilities in home automation systems, such as Cross Site Scripting (XSS).Our current design uses advanced Internet of Things technology integrated into the smart home technology. IoT (Internet of Things) also known as internet of objects which refers to wireless networks between the objects. This technology uses cloud services to provide technological services to the users.

III. Proposed Work

Figure 2 shows the block diagram of the proposed system. We have sensors attached to an ATMEGA 2560 microcontroller. Sensors used are

- Temperature and Humidity Sensor
- Light Sensor
- Door Sensor
- Gas Sensor
- PIR sensor
- Tank Level indicator.

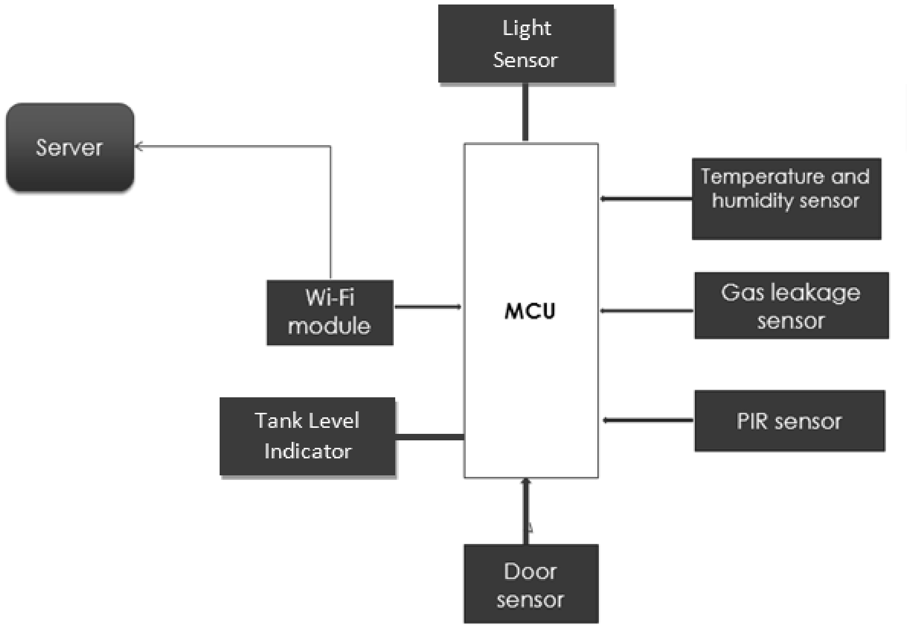

Fig. 2 Block Diagram of the Proposed System

1. HARDWARE

1.1 ATMEGA 2560

The ATmega 2560 provides the following features: 64K/128K/256K bytes of In-System Programmable Flash with Read-While-Write capabilities, 4Kbytes EEPROM, 8Kbytes SRAM, 54/86 general purpose I/O lines, 32 general purpose working registers, Real Time Counter (RTC), six flexible Timer/Counters with compare modes and PWM, four USARTs, a byte oriented 2-wire Serial Interface, a 16-channel, 10-bit ADC with optional differential input stage with programmable gain, programmable Watchdog Timer with Internal Oscillator, an SPI serial port, IEEE® std. 1149.1 compliant JTAG test interface, also used for accessing the On-chip Debug system and programming and six software selectable power saving modes. The Idle mode stops the CPU while allowing the SRAM, Timer/Counters, SPI port, and interrupt system to continue functioning.

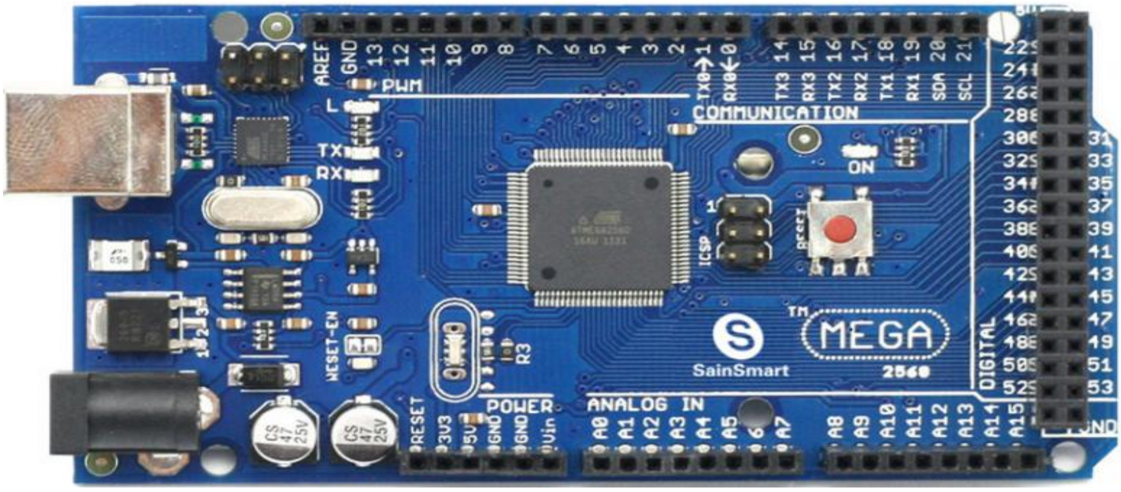

Figure 3 ATMEGA 2560 Microcontroller

The Power-down mode saves the register contents but freezes the Oscillator, disabling all other chip functions until the next interrupt or Hardware Reset. In Power-save mode, the asynchronous timer continues to run, allowing the user to maintain a timer base while the rest of the device is sleeping. The ADC Noise Reduction mode stops the CPU and all I/O modules except Asynchronous Timer and ADC, to minimize switching noise during ADC conversions. In Standby mode, the Crystal/Resonator Oscillator is running while the rest of the device is sleeping. This allows very fast start-up combined with low power consumption. In Extended Standby mode, both the main Oscillator and the Asynchronous Timer continue to run.

1.2 ESP8266 WIFI MODULE

ESP8266 Wi-Fi module is shown in Fig 3. It has a 32-bit Ten silicon 80MHz microprocessor and 4 MB of flash memory. The unit has a built-in support with dedicated pins for UART, SPI and I2C protocols.

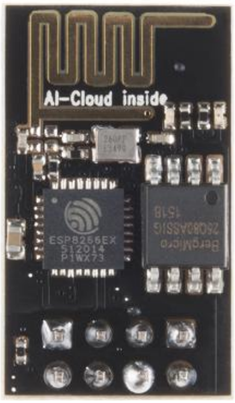

Fig. 4 ESP8266 Wi-Fi Module

1.3 Light Sensor

This is a BH1750 light intensity sensor breakout board with a 16 bit AD converter built-in which can directly output a digital signal. There is no need for complicated calculations. This is a more accurate and easier to use version of the simple photo resistor which only outputs a voltage that needs to be calculated in order to obtain meaningful data. With the BH1750 Light Sensor intensity can be directly measured by the lux meter, without needing to make calculations. The data which is output by this sensor is directly output in Lux (Lx). When objects which are lighted in homogeneous get the 1 lx luminous flux in one square meter, their light intensity is 1lx. Sometimes to take good advantage of the illuminant, you can add a reflector to the illuminant. So that there will be more luminous flux in some directions and it can increase the illumination of the target surface.

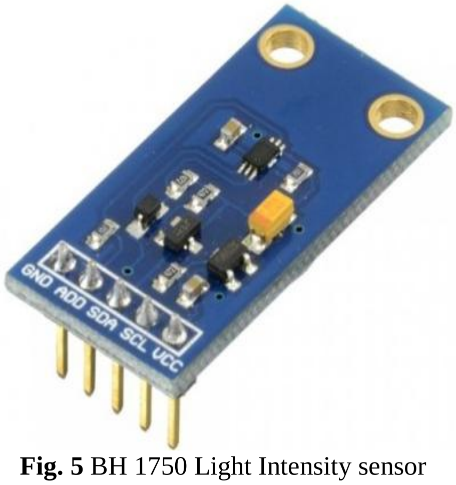

Fig. 5 BH 1750 Light Intensity sensor

The UV Sensor is used for detecting the intensity of incident ultraviolet (UV) radiation. This form of electromagnetic radiation has shorter wavelengths than visible radiation. This module is based on the sensor UVM-30A, which has a wide spectral range of 200nm-370nm.

1.4 Gas *S*ensor

This is a simple to use liquefied petroleum gas (LPG) sensor, suitable for sensing LPG (composed of mostly propane and butane) concentrations in the air. The MQ-6 can detect gas concentrations anywhere from 200 to 10000 ppm .This sensor has a high sensitivity and Fast response time. The sensors output is an Ana log resistance. The drive circuit is very simple; all you need to do is power the heater coil with 5v, add a load resistance, and connect the output to an ADC.

Fig. 6 Gas Leakage Sensor

This sensor module utilizes an MQ-6 as the sensitive component and has a protection resistor and an adjustable resistor on the board. The MQ-6 gas sensor is highly sensitive to LPG, Iso butane, propane and less sensitive to alcohol, cooking fume and cigarette smoke. It could be used in gas leakage detecting equipment's in family and industry. The resistance of the sensitive component changes as the concentration of the target gas changes.

1.5 PIR Sensor Passive Infrared Sensor (PIR)

Passive infrared sensor (PIR) is an electronic device that can measure the transmitted infrared light. The term passive in this regard should be translated that the device does not emit the infrared rays PIR but only passively receive incoming infrared radiation. ”Infra” Wilkins below our ability to detect visually and “Red” because this colour represents the lowest energy level that we see before it becomes invisible (fig).the PIR can be used to detect movements, normally used to detect human movement when passing in or out of range sensor .PIR is a small, cheap, low power, easy to use and durable PIR is basically made of pyro electric sensor that can detect infrared radiation levels.

Fig . 7 PIR SENSOR

PIR sensors allow you to sense motion, almost always used to detect whether a human has moved in or out of the sensors range. . They are often referred to as PIR, "Passive Infrared", "Pyroelectric", or "IR motion" sensors. The PIR sensor range is up to 10 meters at an angle of +15^0 or -15^0.

1.6 Temperature and Humidity sensor SHT25

The SHT25 is a high end version humidity and temperature sensor IC in 6 pin DFN package. It has become an industry standard in terms of form factor and intelligence. This device provides calibrated, linearized sensor signals in digital I2C format. The SHT25 sensor contains capacitive type humidity sensor, band gap temperature sensor and specialized analogue and digital integrated circuit on a single CMOS sensor chip. This yields an unmatched sensor performance in terms of accuracy and stability as well as minimal power consumption.

Fig. 8 Temperature and humidity Sensor

SHT25 I2C Humidity and Temperature Sensor ±1.8%RH ±0.2°C I2C Mini Module. It is high-accuracy humidity and temperature sensor has become an industry standard in terms of form factor and intelligence, providing calibrated, linearized sensor signals in digital, I2C format. Integrated with a specialized analog and digital circuit this sensor is one of the most efficient device to measure the temperature and humidity.

1.7 Door sensor

A magnetic contact switch is basically a reed switch encased in a plastic shell so that you can easily apply them in a door, a window or a drawer to detect if the door is open or closed. The switch that we are going to use has two parts: the switch itself, that usually comes opened and the magnet. When you buy this switch, it also comes with 4 screws, so that you can attach it to your door.

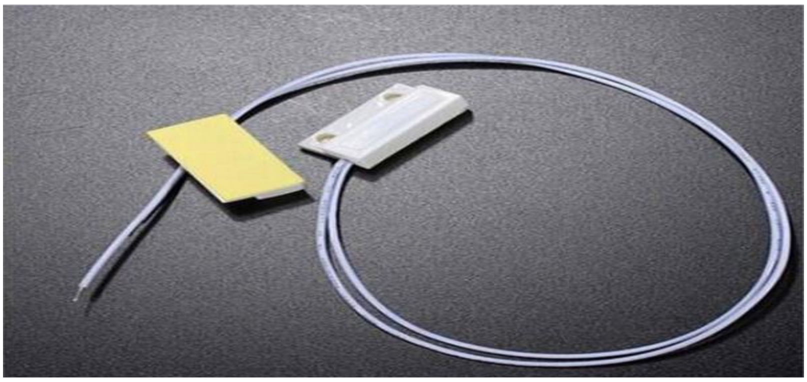

Fig . 9 Door Sensor

1.8 HC SR-04 Ultrasonic Sensor

The HC-SR04 ultrasonic sensor uses sonar to determine distance to an object like bats do. It offers excellent non-contact range detection with high accuracy and stable readings in an easy to use package. From 2cm to 400 cm or 1" to 13 feet. It operation is not affected by sunlight or black material like Sharp rangefinders are (although acoustically soft materials like cloth can be difficult to detect). It comes complete with ultrasonic transmitter and receiver module.

IV. Result

The complete system was designed using the hardware mentioned previously. The coding part is implemented using Arduino IDE. The Arduino Integrated Development Environment or Arduino Software (IDE) - contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions and a series of menus. It connects to the Arduino and Genuino hardware to upload programs and communicate with them.

Programs written using Arduino Software (IDE) are called sketches. These sketches are written in the text editor and are saved with the file extension.ino. The editor has features for cutting/pasting and for searching/replacing text. The message area gives feedback while saving and exporting and also displays errors. The console displays text output by the Arduino Software (IDE), including complete error messages and other information. The bottom right hand corner of the window displays the configured board and serial port. The toolbar buttons allow you to verify and upload programs, create, open, and save sketches, and open the serial monitor. A channel was created at the Thing Speak server to post the data. This posting is possible only with the help of the Write API key, which is private. In this way, we can securely transmit data through the channel.

The results were shown below.

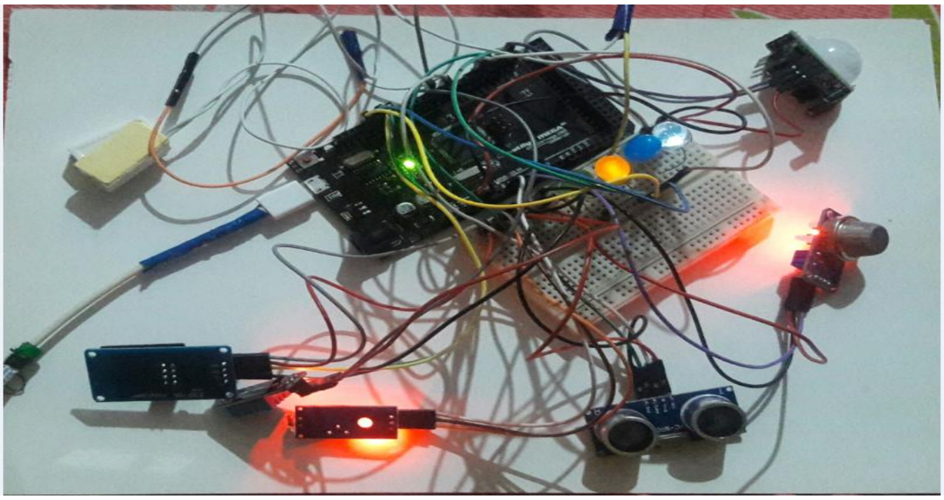

Fig . 10 Kit and It's Output

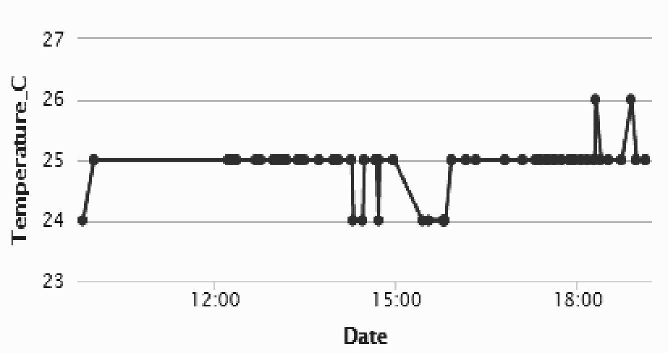

Fig .11 Variation of Temperature in ^{0}C

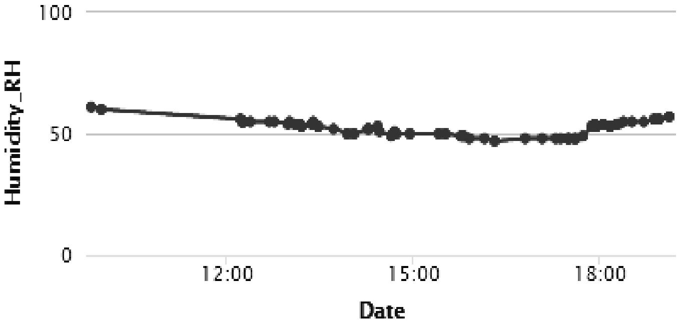

Fig . 12 Variation of Humidity in %RH

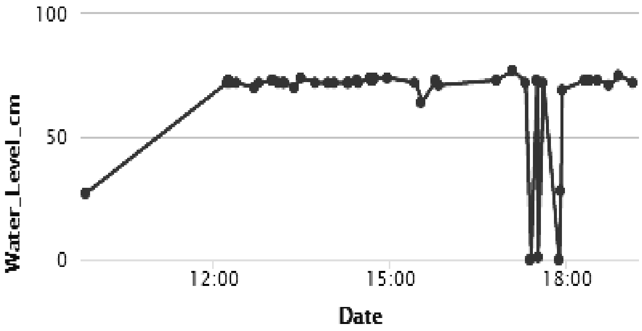

Fig . 13 Water Tank Level

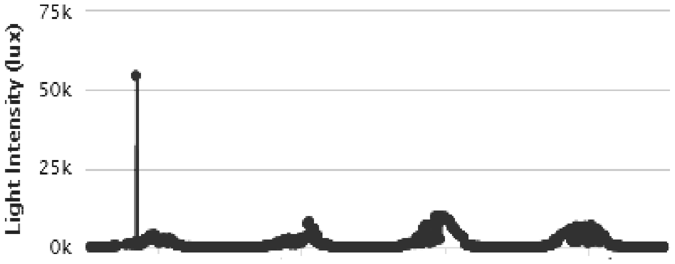

Fig . 14 Variation of Light intensity in Lux

Results shows that the home automation system is functioning as desired and is providing an efficiency greater than 90%. Data about various parameters is stored on cloud and can be accessed from any place around the world. Further a web application or a mobile application can be developed to handle this data and users can view the situation at home and can lead a happier and safe life.

V. Conclusion

In this work, we have designed, developed and tested a smart home automation using Internet of Things architecture. Various security and monitoring measures were incorporated and then integrated into the design. System monitors various parameters like Temperature, Humidity, Water Tank Level, Intrusion detection using PIR sensor. Automation of light control and water level management is achieved using sensors. The system uses ESP8266 Wi-Fi module for communication purpose. This module will establish a connection with a remote server and it will store the data on a server. Thing Speak, a free server was used to develop the prototype. Results show that the system is working accurately and is stable over a long period of its operation. This solution is economic and hence feasible to implement at homes, industries and work places.

References

[1] Brand, S, How Buildings Learn, New York, Viking, 1994.

[2] R. E. Grinter, N. Ducheneaut, W.K. Edwards, M. Newman, “The work to make a home network work,” in Proc. of Ninth European Conference on Computer-Supported Cooperative Work (ECSCW 05), pp. 469-488, 2005.

[3] M. Chetty, J.-Y. Sung, R. E. Grinter, “How Smart Homes Learn: The Evolution of the Networked Home and Household,” Lecture Notes in Computer Science, vol. 4717, pp. 127-144, 2007.

[4] Greichen, J.J., “Value based home automation or today's market,” IEEE Transactions on Consumer Electronics, vol. 38, no. 3, pp.34-38, Aug. 1992.

[5] “The X10 Specification,” X-10 (USA) Inc., 1990.

[6] “ZigBee Specifications,” ZigBee Alliance, version 1.0 r13, Dec. 2006.

[7] “LonTalk Protocol Specification Version 3.0,” Echelon Co, 1994.

[8] “EIA-600 CEBus Standard Specification,” EIA, 1992.

[9] A.J. Bernheim Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, C. Dixon, “Home automation in the Wild: Challenges and Opportunities,” in CHI ’11 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 2115-2124, 2011.

[10] K. Madhuri, B. L. Sai, B. S. Sirisha, “A Home Automation System Design Using Hardware Descriptive Tools,” International Journal of Engineering Research & Technology, vol. 2, no. 7, Jul. 2013.

[11] E.M.C Wong, “A Phone-Based Remote Controller for Home and Office Automation,” IEEE Transactions on Consumer Electronics, vol. 40, no. 1, pp.28-34, Feb. 1994.

[12] A. ElShafee, K. A. Hamed, “Design and Implementation of a WiFi Based home automation System,” World Academy of Science, Engineering and Technology, vol. 6, 2012.

[13] M. Danaher, D. Nguyen, “Mobile Home Security with GPRS,” in proceedings of the 8th International Symposium for Information Science, Oct. 2002.

[14] A. Alheraish, “Design and Implementation of Home Automation System,” IEEE Transactions on Consumer Electronics, vol. 50 , no. 4, pp.1087-1092, Nov. 2004.

[15] V. Singhvi, A. Krause, C. Guestrin, James H. Garrett Jr., H. Scott Matthews, “Intelligent Light Control using Sensor Networks,” in Proceedings of the 3rd international conference on Embedded networked sensor systems, SenSys '05, pp. 218-229, 2005.

[16] A. Gaddam, “Development of a Bed Sensor for an Integrated Digital Home Monitoring System,” IEEE International Workshop on Medical Measurements and Applications, pp. 33-38, May 2008.

[17] U. Saeed, S. Syed, S.Z. Qazi, N.Khan, A.Khan, M.Babar, “Multi-advantage and security based home automation system,” 2010 Fourth UKSim European Symposium on Computer Modeling and Simulation (EMS), pp.7-11, Nov. 2010.

[18] C. Karlof, D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures”, Ad Hoc Networks, vol. 1, pp. 293–315, 2003.

[19] Y. Hu, A. Perrig, D. Johnson, “Wormhole attacks in wireless networks”, IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 370–380, Feb. 2006.

[20] J. Wright, “Practical ZigBee Exploitation Framework”, Toorcon, Oct. 2011.

[21] Z. Feng, J. Ning, I. Broustis, K. Pelechrinis, S.V. Krishnamurthy, M. Faloutsos, “Coping with Packet Replay Attacks in Wireless Networks,” 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, pp. 368-376, Jun. 2011.

[22] B. Fouladi, S. Ghanoun, “Security Evaluation of the Z-Wave Wireless Protocol,” Black hat USA, Aug. 2013.

[23] T. Oluwafemi, S. Gupta, S. Patel, T. Kohno, “Experimental Security Analyses of Non-Networked Compact Fluorescent Lamps: A Case Study of home automation Security,” Workshop on Learning from Authoritative Security Experiment Results, pp. 13 – 34, Oct. 2013.

[24] A. Verrotti, D. Trotta, C. Salladini, G. Corcia, G. Latini, R. Cutarella, F. Chiarelli, “Photosensitivity and epilepsy: a follow-up study,” Developmental Medicine & Child Neurology, vol. 46, no. 5, pp. 347-351, May 2004.

IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) is UGC approved Journal with Sl. No. 5016, Journal no. 49082.

K.Sreeja. “A Novel Database Assited System for Smart Living Using Iot.” IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), vol. 12, no. 4, 2017, pp. 36–44.