IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 1)
Available online at: www.ijariit.com

Ensure the securities in IoT for home monitoring system

Kaviya S.
kaviyaoct20@gmail.com
KPR Institute of Engineering and Technology, Coimbatore, Tamil Nadu

Divya Lakshmi R.
ldivya892@gmail.com
KPR Institute of Engineering and Technology, Coimbatore, Tamil Nadu

Jenifa G.
gjenifa@gmail.com
KPR Institute of Engineering and Technology, Coimbatore, Tamil Nadu

ABSTRACT

Smart building using IOT technique is used to maintain a home in a smarter way. In order to enhance the security in the home the various combinations of the sensor are used. In that PIR and MQ-6 sensors plays a major role. The data from these sensors are sent to the Arduino board and get stored in the cloud. In this paper home monitoring system along with intrusion, detection technique is used. For data security, wireless sensor network (WSN) playa a major role. To facilitate data encryption, a method namely Triangle Based Security Algorithm (TBSA) based on an efficient key generation mechanism was proposed.

Keywords*— IoT technique, Intrusion detection, Data security, Wireless Sensor Network, Triangle-based security algorithm*

1. INTRODUCTION

The smart building using IOT is a wireless home security project. In today's world security and safety is essential for home. If the sensor found any intruders, then it will send an alert message to the concerned people. To provide security the many sensors are used and for faster data transmission the ESP8266 sensor plays a major role, which is used to control and monitor the system. To provide security for the transmitted data the Triangle Based Security Algorithm (TBSA) is used. In this proposed system the sensors used are highly reliable and it will consume very less power in comparison with the existing system. IoT involves extending internet connectivity beyond devices such as desktops, laptops, smartphones and tablets. In SHAS schema, connecting a TV or a refrigerator to the Internet might be considered as a normal scenario, since it would make our life easier. However, the single fact of connecting such node to the IoT world might generate a potential vulnerability since a hardening standard is still not in place to protect such devices. In addition, the risk arises as the SHAS is being used to handle physical security services, such as opening doors or preventing burglars from entering a place.

2. SECURITY APPROACHES

A monitoring system is built for the home automation system: In Shetel and Agarwal IOT paper (2016) explain internet connectivity for all kind of devices and physical objects in real time system. This paper used to manage multiple jobs without any limitations.

In Lee(2017) explains in their paper the explains the physical objects in IOT which contains the embedded technology helping in developing machine to machine or man to machine communication. This paper gives data about the environment parameters taken from the stand-alone system.

In Chou (2017) describes in their paper a home automated system has a remote-controlled operation. This paper tells about the problem in their installation, finding out the various solutions through different network technologies. The Home Automation System (HAS) requires heterogeneous, an eternal and distributive computing environment's careful study to develop the suitable HAS.

3. PROPOSED SYSTEM

In this paper, we are proposing a smart home monitoring system with various sensors. The PIR sensor is used to sense the movement of people entering the door. The Arduino acts as a brain of the system and it will receive all the data sent by the sensors. The Arduino board transfers the collected data to the cloud for storage. During data transmission, to prevent the data from intruders an algorithm named Triangle Based Security Algorithm is used. This algorithm provides confidentiality and integrity for the data so that the data can be prevented from the third party.

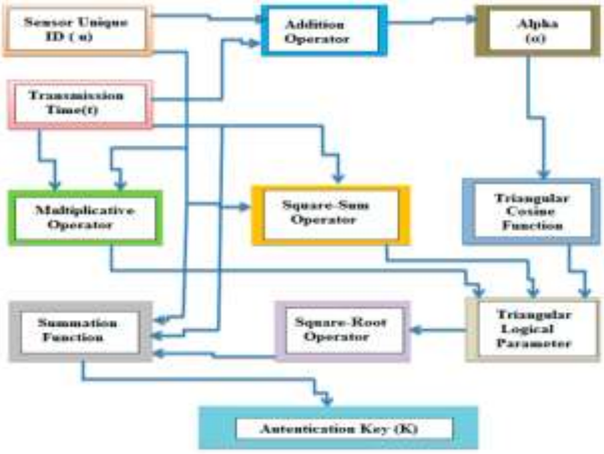

Fig. 1: Key generation mechanism for TBSA

3.1 Sensors used

3.1.1 PIR Sensor: A **PIR** sensor is an electronic sensor. They are used as **motion** detectors. A PIR sensor is used to sense the movement of people, animals and other objects and sends the data to the Arduino. A PIR sensor measures infrared light from objects. The Crystal material is placed at the centre of a rectangle on the face of the sensor. This sensor also detects a human being moving around within **approximately 10m** from the sensor. This is an average value, as the actual detection range is between 5m and 12m.PIR is fundamentally made of a pyroelectric sensor, which can detect levels of infrared radiation.

3.1.2 MQ-6 Sensor: The MQ6 sensor is a liquefied petroleum gas sensor. This sensor can detect gas leakage in consumer and industry applications, this sensor is suitable for detecting LPG, **iso-butane**, propane, LNG. The MQ-6 sensor can detect gas from 200-10000 ppm. This sensor is a highly sensitive sensor and fast response time.

Some of the features of MQ-6:

•High Sensitivity to LPG, ISO-butane, propane
• Small sensitivity to alcohol, smoke
• Fast Response Time: <10s
• Simple drive circuit
• Heater Voltage: 5.0V

3.1.3 ESP 8266 Wi-Fi Module: This will be used to integrate the system on to the cloud and facilitates storage and analysis of data collected. The ESP8266 Wi-Fi Module is a self-contained SOC with integrated TCP/IP protocol stack that can give any microcontroller access to your Wi-Fi network. The ESP8266 is capable of either hosting an application or offloading all Wi-Fi networking functions from another application processor.

3.2 Hardware requirements

3.2.1 Arduino Uno: It will act as a brain of the system and processes the data from the sensor and facilitates the switching ON/OFF of the electrical appliances. Arduino is an open-source electronics platform based on easy-to-use hardware and software. Arduino boards are able to read inputs - light on a sensor, a finger on a button, or a Twitter message - and turn it into an output - activating a motor, turning on an LED, publishing something online.it consists of both a physical programmable circuit board and a piece of software, or IDE (Integrated Development Environment) that runs on your computer, used to write and upload computer code to the physical board.

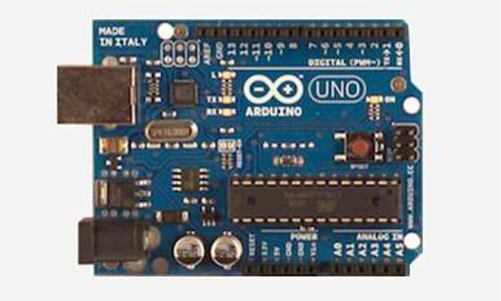

Fig. 2: Arduino UNO

4. SYSTEM DESIGN

Triangle-Based Security Algorithm (TBSA) pretends to protect data that is being transmitted through an insecure channel. This algorithm assigns keys to all participant sensors. It also uses tracking sequence values to speed authentication, prevent replay attacks, identify source nodes, and guarantee data protection. In addition, validating SSID along with password provides an extra level of data protection. Once the node has executed all authentication steps, it could generate a cypher text using TBSA. Moreover, recognizing users and devices as well as access control policies, the system prevents unwanted users from accessing the system. Finally, in this system, data would be transmitted to the Arduino device and if there is a match between channel and field ID, the destination node should be able to decrypt the message. TBSA is based on the triangular logical function.

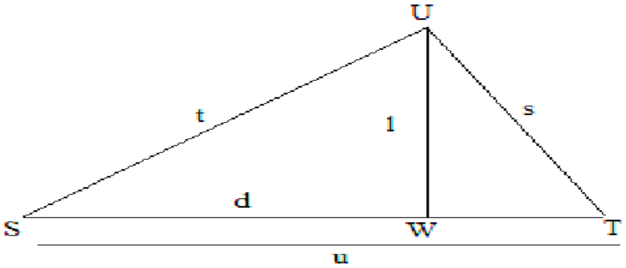

Fig. 3: TBSA Triangle

4.1 Intrusion in the cloud

Many IoT systems use a cloud for data analysis, storage, and management. Because cloud providers are responsible for security. A cloud infrastructure operated by the service provider uses extensive virtualization techniques, which enables easier to utilize the resources. Cloud infrastructure working in Internet protocols, which may encourage potential attackers. While part of the responsibility lies with the cloud provider, device manufacturers are responsible for the end user.

5. CONCLUSION

The purposed system helps to provide a complete secured building by providing features such as intruder alert, automating electronic item usage. The sensors used here are of low cost. The sizes of the devices are also manageable which makes the purposed system cost-effective. Secured IoT-based home automation applications using WSNs. In WSNs, because of the limited power of sensor nodes, effective key generation mechanism which could accomplish all major data security requirements and consumes less processing time for data encryption is well needed. A security algorithm, namely TBSA is based on a simple and efficient key generation procedure. The proposed IoT integrates low power ESP 8266 and the proposed TBSA in WSNs with internet to provide additional benefits of increased coverage range and capability of supporting a large number of sensor nodes due to usage of low power ESP 8266, it also consumes less processing time for data encryption because of the utilization of the proposed TBSA algorithm.

6. REFERENCES

[1] Rosslin John Robles and Tai-hoon Kim, “Review: ContextAware Tools for Smart Home Development”, International Journal ofSmart Home, Vol.4, No.1, January 2010

[2] Hitendra Rawat, Ashish Kushwah, Khyati Asthana, AkankshaShivhare, “LPG Gas Leakage Detection & Control System”, NationalConference on Synergetic Trends in engineering and Technology(STET-2014) International Journal of Engineering and technical research ISSN: 2321-0869, Special Issue

[3] Nicholas D., Darrell B., Somsak S., “Home Automation using cloud Network and Mobile Devices”, IEEE Southeastcon2012, Proceedings of IEEE. [14] Chan, M., Campo, E., Esteve, D., Fourniols, J.Y., “Smart homescurrentfeatures and future perspectives,” Maturitas, vol. 64, issue 2, pp.90-97, 2009

[4] Savitha, S., and S. Yamuna. "Implementation of AES algorithm to overt fake keys against counter attacks." In Computer Communication and Informatics (ICCCI), 2016 International Conference on, pp. 1-5. IEEE, 2016.Plagiarism Check Report.

[5] Alexandru-Corneliu Olteanu*, George-Daniel Oprina*, Nicolae ğăpuú* and Sven Zeisberg," Enabling mobile devices for home automation using ZigBee".2013 19th International Conference on Control Systems and Computer Science

[6] Luigi Coppolino, Valerio D'Alessandro, Salvatore D'Antonio, Leonid Lev † and Luigi Romano, "My Smart Home is Under Attack" 2015 IEEE 18th International Conference on Computational Science and Engineering.

[7] Makkad, Ritu Kaur, and Anil Kumar Sahu. "Novel design of fast and compact SHA-1 algorithm for security applications." In Recent Trends in Electronics, Information & Communication Technology (RTEICT), IEEE International Conference on, pp. 921-925. IEEE, 2016.

[8] Ratna, Anak Agung Putri, Prima Dewi Purnamasari, Ahmad Shaugi, and Muhammad Salman. "Analysis and comparison of MD5 and SHA-1 algorithm implementation in Simple- O authentication based security system." In QiR (Quality in Research), 2013 International Conference on, pp. 99-104. IEEE, 2013.

[9] Bhanot, Rajdeep, and Rahul Hans. "A review and comparative analysis of various encryption algorithms. "International Journal of Security and Its Applications 9, no. 4 (2015)