2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE) 978-1-7281-4142-8/20/$31.00 ©2020 IEEE 10.1109/ic-ETITE47903.2020.137

Wireless Home Automation Communication and Security with Internet of Things

Isai U
School of Information Technology and Engineering
VIT,Vellore,Tamilnadu,India.
isaiuthiyan22@gmail.com

Karthikeyan G
School of Information Technology and Engineering
VIT,Vellore,Tamilnadu,India
karthikeyan.g2016@vitstudent.ac.in

Harideesh R
School of Information Technology and Engineering
VIT,Vellore,Tamilnadu,India
harideeshr1998@gmail.com

***Abstract*: This technology provides new and exciting opportunities to increase the property of devices at intervals the house for the aim of home automation. Mobile devices are ideal for providing a program to a home automation system due to its wide array of movability and capabilities. They'll communicate with a home automation network through an internet entree, however cannot communicate directly with devices within the network, as these devices usually implement low power communication protocols, like Zig-Bee, Wi-Fi, etc. During this project we are geared towards dominant home appliances. The device uses Wi-Fi because the communication protocol and Raspberry Pi acts as a server system. We tend to supply a simple interface for the device that allows the user to interact with the Raspberry Pi server. The servers are interfered with a relay board that controls the devices running within the house. The server communicates with the individual relay. By this we provide a reliable and price effective home automation system.**

Keywords— Zig-Bee, Wi-Fi, Raspberry Pi server.

I. INTRODUCTION

The "home automation" conception has existed for several years. The term "smart home", "intelligent home" has been used and has been wont to introduce the conception of networking devices and devices within the home. Home Automation Systems (HAS) represents an excellent analysis chance in making new fields in Engineering and Computing. The HAS includes centralized management of lighting, appliances, gates and doors and alternative systems' security controls to produce improved, comfort, energy potency and security systems. HAS is turning into common these days and chop-chop enters this rising market. However, end-users, particularly the disabled and aged, don't invariably settle for these systems.

Due to the advancement of wireless technology, many various connections are introduced like GSM, local area network and Bluetooth. each association has its own unique Specifications and applications. local area network is being chosen from among the four in vogue wireless connections usually enforced inside the HAS project, with its applicable. This could indirectly cut back the worth of this system.

The project advances the design of home automation and security systems exploitation the credit size laptop. Rasp be choices a mini laptop, that's further with its GPIO pin where totally different components and devices is also connected. Raspberry Pi's Government Printing workplace register is utilized for output functions. House appliances unit of measurement connected to the power strip any as a result of the input / output port of the Raspberry Pi and their position reaches the Raspberry Pi. The automaton running OS in Associate in the phone connected to the network can access the standing of home devices through associate application. It presents the design and implementation of automation systems which is able to monitor and management home devices via automaton phones or tablets.

II. DESCRIPTION

Today people are looking at ways and means to improve their lifestyles using modern technologies which are the available fields. Any new feature or hope device that promises to enhance their lifestyles is grabbed by consumers. Such facilities and equipment are added, it is inevitable to have easy and convenient ways and means to control and operate these devices. Traditional wall switches are located in different parts of a house and thus require manual operation to turn these switches on or off to control various devices. It almost becomes impossible to keep track of the devices that are running and also to monitor their performance.

IMPORTANCE

The unskillfulness of operative ancient wall switches are often inundated by victimization numerous home automation systems .The power loss are often reduced and also the work force needed for home automation is far below ancient strategies. Raspberry Pi primarily based home automation systems are often a lot of economical, providing easy operation. Electric

978-1-7281-4142-8/$31.00 ©2020 IEEE

Authorized licensed use limited to: Auckland University of Technology. Downloaded on June 07,2020 at 03:51:14 UTC from IEEE Xplore. Restrictions apply.

power provides protection from short circuits victimization standard wall switches to work hundreds. By victimization home automation systems, we are able to save plenty of your time to work home appliances from anyplace.

III. PROPOSED SYSTEM

In this project we use a Cloud based service called"Think Speak". This platform provides North American country with the tools necessary for aggregation, Analyzing and Triggering events. For our Home Automation, we arrange the user with the data of what proportion of power is consumed by every element running for a selected time within the house that is machine-controlled and can also be monitored through mobile phones. So giving the user associate energy economical and economical plan of the way to use the natural philosophy within the house.

CHALLENGES

1. *Sub systems not integrating*

This is a drag which will have an effect on all systems from an easy plugin device to a centrally controlled Raspberry.

2. *Finding the right requirement for user*

To overcome this drawback, we've got integrated each automatic managements of Raspberry or Illumination control by Rasp Controller App.

3. *Python version for cryptography*

Python is employed for this wherever the version keeps change and can't follow up with the speed of the update.

4. *Code construction*

One of the foremost frustrating issues is that the prevalence of long warnings and errors throughout the development of our new sensible home project.

ASSUMPTIONS

User and management unit can establish communication via WLAN. All service charges from the applicable service supplier apply. Controlled devices should have associate electrical interface to regulate the controlled microcontroller.

ARCHITECTURE SPECIFICATIONS

HARDWARE INTERFACE

- The Raspberry Pi is connected to the portable computer with local area network.
- The devices specifically ultrasonic sensor, PIR motion Detection device.
- Lights, Fans, alternative appliances area unit connected to the Raspberry's board pins.

SOFTWARE CONTROL COMPONENETS

Coding is finished within the Raspberry desktop as Python: once an individual lights up a house and therefore the fan mounted in its place should be turned on mechanically till it's gift within the area.

The runtime of every element currently used is uploaded to the Think Speak cloud, that stores the info. The analysis is performed for information and functions that area unit iterated supported the given conditions. In our project here, the home-owner ought to set a monthly budget to pay the electricity bill. Currently that the present usage is bigger than or higher than the set price, the person ought to receive a notification on the mobile to cut back the facility. If the individual grants a lot of permissions to the parts, it'll shut itself down if the budget is exceeded. The management of the parts can even be created manual by the user and management the Rasp Controller app. Data analysis and actions can even be performed in manual management mode. The hardware required for the application would be Raspberry pi 3, LED, DC motor, PIR motion sensor, Ultrasonic sensor and few connecting wires. The software requirements would be the VNC viewer, ThinkgsSpeak cloud and Rasp controller.

INTERNET OF THINGS DESIGN METHODOLOGIES

STEP:1 – PURPOSE AND REQUIREMENTS

Purpose: A home automation system that enables remote of the house lights employing internet application permits.
Practices: Home automation systems should have auto and manual modes. In motorcar mode, the system measures the extent of sunshine within the area and switches on the sunshine once it's dark.
Information analysis required: The system should perform native analysis of the information.
Application preparation required*:* The appliance should be deployed domestically on the device, however should be remotely accessible.
Security required: The system should have basic user authentication capabilities.

STEP:2 – PROCESS SPECIFICATION

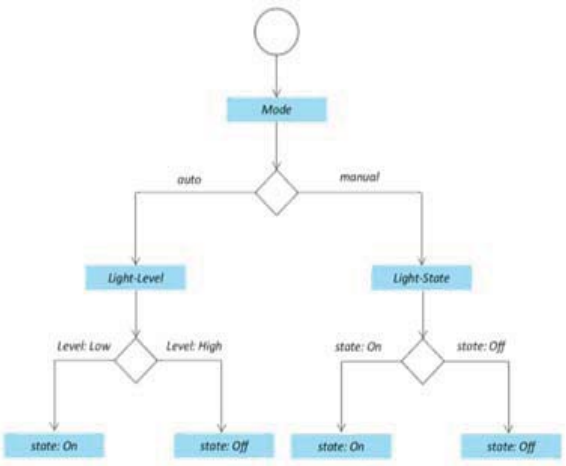

Fig:1 process specification

Authorized licensed use limited to: Auckland University of Technology. Downloaded on June 07,2020 at 03:51:14 UTC from IEEE Xplore. Restrictions apply.

STEP:3 – SERVICE SPECIFICATION

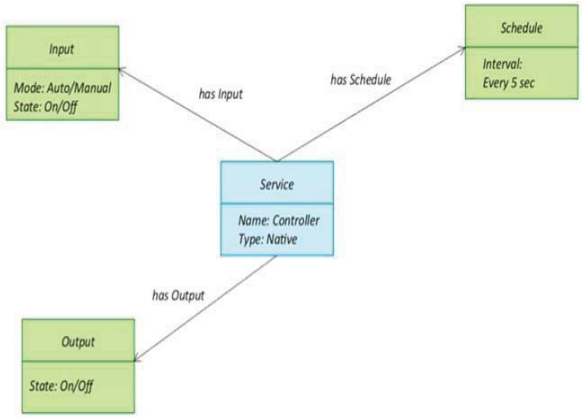

Fig:2 service specification

STEP:4 – INTERNET OF THINGS LEVEL SPECIFICATION

This project is a Level 4 project

STEP:5 – FUNCTIONAL VIEW SPECIFICATION

Device (monitor and control): Raspberry Pi three, Thing Speak and Rasp Controller robot App.
Communication: wireless fidelity.
Services: remote of devices and observation usage.

STEP:6 - OPERATIONAL VIEW SPECIFICATION

Service Hosting Options: Authentication by Raspberry and Rasp controller.

Storage Options: ThingsSpeak info.

EquipmentOptions:

1.Computing Device: Raspberry Pi three.

2.Sensor: Ultrasonic, Motion.

3.Actuators: Lights and Fans.

Application Hosting Options: Thing Speak Application.

IV. SECURITY THREATS

Wireless device networks unit currently being wide util ized in wild life studies producing observance units. Wireless device networks have limitations within the areas of communication and computing. They're conjointly hospitable numerous attacks thanks to their preparation nature. Once the device node is being captured by the attackers, malicious code will simply be accepted by the network within the place of the first code.

The limitations within the device networks area unit are from nodes, network and physical aspects. Node limitations in device networks area unit are due to their heterogeneous nature.
And conjointly they're hospitable physical destruction s ince they're deployed in such environments thanks to their preparation nature.

In hostile environments, device networks area unit hospitable destruction due
to their preparation nature. So as to rectify this issue, nodes of upper value ought to be used. The security and dependableness of the device networks area unit is being challenged by their unplanned nature. The device networks area unit deployed in physically areas, creating it liable to numerous attacks. Thus, distinctive security methodologies area unit needed to beat these challenges. Security in wireless device networks will be fixed up by achieving the protection goals like confidentiality, integrity, handiness and credibility.

- ***Confidentiality*** is once the message shared is hid from a passive assailant.

- ***Integrity*** is once the message shared isn't being tampered, altered or modified within the method.
  Authenticity is checking if the message is being received from the licensed node or not.

- ***Availability*** is ensuring that the network is usually prepared for sharing the message.

- ***Virus:*** Mobile phone is end device in WAP architecture, which is vulnerable to virus attacks which is a gateway to get the system spoiled.

- ***Physical security:*** As discussed above phone is the weakest link in the system, sensitive data's are stored in the end device so the possibility of theft and sophisticated operating system will make the whole system more vulnerable.
  We can solve these problems by upgrading WAP gateway, switching to trusted gateway and using PIN code to access phone.

SOLUTIONS FOR SECURITY THREATS

Security Solutions for Wireless Sensor Networks (WSNs)

Some solutions related to wireless sensor networks are as follows:
1. Shared key: A security feature that tends to realize a good deal of concentration in WSNs is that the key management area. WSNs are found to be unique during this feature thanks to their size, mobility and lack of power. Traditionally, using one in every of several public-key protocols completes key installation. Usually by implementing an easy key infrastructure, protection from external attacks for any network is taken care of. However, it's known that a worldwide key doesn't provide flexibility to any network, and therefore the pairwise secret is not a scalable solution.

Authorized licensed use limited to: Auckland University of Technology. Downloaded on June 07,2020 at 03:51:14 UTC from IEEE Xplore. Restrictions apply.

2. Protected grouping: WSNs have an outsized number of small nodes which are compact and automatic devices. To accomplish a specific task, it's important that group members are ready to communicate safely with one another, whether or not overall security is additionally in use. Exceptions to the answer are made when static groups have more powerful nodes to safeguard a member.

3. Encryption: Sensor networks run on inherently unintentional wireless channels in most public or wild areas. Thus, it is negligible for the device to add messages sideways or even across the network.

4. Secure Data Aggregation: Sensor networks and data aggregation techniques tend toward multiple attacks, including denial of service attacks. The foremost important problem within the network is data traffic which is caused by the rise in data transfer. To cut back overhead costs and network traffic, the sensor nodes get the entire measurement before sending it to the bottom station. This sort of knowledge is allocated to an attacker. The reliability of the generated data is affected if an opposing node has control and chooses to ignore the report or produce a false report. Consequently, the network as a full must be considered. The most objective during this area is to use flexible functions which will be able to search and report forged reports through demonstrating the authenticity of the information in a way. However, rise during this area should still be needed, like the number of solutions generated by the interactive algorithm.

5. SPINS: SPINS has many building blocks due to which it provides many security properties such as data authentication, data freshness, semantic security, reduced communication overhead, and re-security.

6. Tiny Sec: Link Layer Security Architecture: Tiny Sec can be included in sensor network applications because they are lightweight and are a common security package, and therefore it is included in the official Tiny OS release.

TABLE:1 threats and solutions

THREATS	SOLUTIONS
Physical attack and reverse engineering	Tamper resistant mechanism
Data integrity problem	Detects security threats in data integrity then adjusts to environment with censored changes detected while exploiting metrics for security
Sybil attacks	Keep tracking the number of clones
Sinkhole attack	By avoiding congestion
Malicious node	By detecting malicious node
DDOS attack	Packet marking, filtering
Attack on network availability	Secure routing
Eavesdropping	Secure relay communication
Cryptanalysis attack	Enhanced two way user authentication scheme
Spoofing identity	Proper authentication and protecting sensitive data
Tampering with data	Proper authentication, hashing, digital signature
Repudiation	Digital signature and timestamp
Denial of service	Authentication and authorization, backup server
Information disclosure	Encryption and decryption, authorization

PRIVACY

1. Identification: Identification refers to the danger of associating a (persistent) symbol, like associate address and name or a nom de guerre of any kind, with info a few person and him. This threat lies in linking associate identity to a selected privacy, violates context, and additionally activates and facilitates alternative threats. as an example, the identification and chase of people or the gathering of assorted knowledge sources. Identity threat is presently most rife withinthe scientific discipline introduce backendservices, wherever massive am ounts of information square measure collected at a central location outside the subject's management.

2. *Localization and Tracking:* Localization and chase indicate the danger of determinant and documenting a personality's location through time and area. chase needs identification to bind continuous localizations to a private. Currently, chase is feasible through varied means that like web traffic, GPS or cellular phone location. Most concrete privacy violations associated with this threat are known, as an example GPS stalking, speech act of private info. In immediate physical proximity, localization and chase typically don't cause a breach of privacy, as an example, anyone within the neighborhood will directly examine the subject's location. Localization and chase so seem primarily as a threat within the scientific discipline section once location traces square measure created on the rear finish outside the subject's management. the most challenges moon-faced in localization and chase square measure passive info concentration, management of shared location knowledge in indoor environments, and awareness of chase privacy protection protocols for communication with Internet of Things systems.

3. Privacy violating interaction and presentation: In this danger, personal details square measure distributed through a public medium then unconcealed to undesirable people. several Internet of Things applications like producing, infrastructure, medical and health care systems, etc. It's conceivable that users square measure given the assistance of good things within the atmosphere. As an example, lighting technology and showing videos through television or desktop screens. In distinction, users dominate the system in another intuitive technique with the employment of good things within the atmosphere. Nonetheless, several intergovernmental and organizing processes square measure in public. This so causesprivacy downside once secret info is chan ged between the user and also the system. As an example, in good cities, someone might question the route to a selected hospital.

Authorized licensed use limited to: Auckland University of Technology. Downloaded on June 07,2020 at 03:51:14 UTC from IEEE Xplore. Restrictions apply.

PRIVACY PRESERVATION SOLUTION

Access management:Access control is one in all the viable solutions utilized in combination with cryptography and privacy awareness.

Privacy awareness and context awareness: Privacy awareness solutions are targeted totally on applications from people WHO give a basic privacy awareness to their users that sensible devices, like wearable fitness devices, smart TVs, and health monitors.Systems will collect personal knowledge concerning them. for instance, in recent analysis, a framework referred to as SeCoMan was planned to treat users as a trusty third party as a result of applications might not be thought-about sufficiently reliable with location data that's managed.

V. CONCLUSION

The proposed home automation system works efficiently using Raspberry Pi, with which cloud services called Think Speak are associated. The system is ready to spot the ability consumed by various devices by taking the run time of every device and sent to Think represent its analysis. The system can identify if there has been any increase in power consumed by the devices by notifying users by sending a tweet via Think Speak. Internet of Things has numerous benefits for businesses, educational sectors moreover as individuals. Information in Internet of Things is transmitted through RFID tags or sensors that carry sensitive information that's shielded from any unauthorized access. This paper discusses the key threats and their associated solutions in Internet of Things by identifying various areas susceptible to security and privacy attacks. As a future approach to protecting Internet of Things, better security frameworks will be developed that may address privacy issues the least bit boundaries. More research is required to develop and style appropriate security mechanisms that are resilient to numerous styles of attacks.

REFERENCES

[1] Zia, T., & Zomaya, A. (2006, October). Security issues in wireless sensor networks. In *2006 International Conference on Systems and Networks Communications (ICSNC'06)* (pp. 40-40). IEEE.

[2] Du, X., & Chen, H. H. (2008). Security in wireless sensor networks. *IEEE Wireless Communications*, *15*(4), 60-66.

[3] Pathan, A. S. K., Lee, H. W., & Hong, C. S. (2006, February). Security in wireless sensor networks: issues and challenges. In *2006 8th International Conference Advanced Communication Technology* (Vol. 2, pp. 6-pp). IEEE.

[4] Khan, M. A., & Salah, K. (2018). Internet of Things security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395-411.

[5] Singelée, D., & Preneel, B. (2003). The wireless application protocol (WAP). *Cosic Internet Report*.

[6] Debbabi, M., Laverdière, M. A., Mourad, A., & Tlili, S. (2008). Wireless Applications: Middleware Security.

[7] Burg, A., Chattopadhyay, A., & Lam, K. Y. (2017). Wireless communication and security issues for cyber–physical systems and the Internet-of-Things. *Proceedings of the IEEE*, *106*(1), 38-60.

[8] HFeng and W. Fu. "Study of recent development about privacy and security of the Internet of Things.' In IEEE International Conference on Web Information Systems and Mining, 2, pp. 91–95, 2010.

[9] K. Raju and V. Bapauji. "Internet of Things (IoT): Security and privacy threats." In IEEE International Conference Robot Autom, 2016. [Online]. Available: https://www.researchgate.net/publication/305302451 [March 26, 2018]

[10] N. Aleisa and K. Renaud, "Privacy of the Internet of Things: A Systematic Literature Review (Extended Discussion)," unpublished. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1611/1611.03340.pdf [March 26, 2018]

[11] M. Daud, Q. Khan, and Y. Saleem. "A study of key technologies for IoT and associated security challengers." In International Symposium on Wireless Systems and Networks, 2017. [Online]. Available: https://ieeexplore.ieee.org/document/8250042 [March 26, 2018]

[12] Harpal, G. Tejpal and S. Sharma. "A survey article on attacks and security goals in Wireless Sensor Networks." In Second International Conference on Communication and Electronics Systems, 2017, pp683-686.

[13] A. Tyagi, J. Kusshwah and M. Bhalla. "Threats to security of Wireless Sensor Networks." In Seventh International Conference on Cloud Computing, Data Science & Engineering – Confluence, 2017, pp685-65

Authorized licensed use limited to: Auckland University of Technology. Downloaded on June 07,2020 at 03:51:14 UTC from IEEE Xplore. Restrictions apply.