ISSN: 0976-3104

SPECIAL ISSUE: (Emerging Technologies in Networking and Security (ETNS)
Devi et al.

THE IIOAB JOURNAL

ARTICLE OPEN ACCESS

INTERNET OF THINGS: A SURVEY ON PRIVACY AND SECURITYFOR SMART HOMES

G. Devi*, R. Rohini, P. Suganya

Dept of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Tiruchengode, Tamilnadu, INDIA

ABSTRACT

***Aim:** Smart Home is one of the applications of Internet of things, in networking side Internet of Things is popular one. The smart home environment is a building block of the future Internet, and many homes are fitting "smarter" by using Internet of Things (IoT) technology to improve home security, energy efficiency and comfort. Latest techniques are used in smart home automation system like automatic door open, automatic light off/on using RFID sensors, etc. The need of home safety is specifically when the elderly person is alone or Children are with baby-sitter and servant. The home attack crimes are done by breaking the door or window and continuously monitoring the home is a challenging one. To Overcome this crimes using door locking sensor is placed in the door and this sensor is to capture the face who are all coming inside the home and the faces are captured. The face will be stored in the cloud and the captured face is verified by the owner of the home. To review the latest technologies are used in smart home automation system security methods in door locking system.*

Published on: 2nd -December-2016

KEY WORDS

Internet of Things (IoT), Smart Home Automation System (SHAS), Smart Lock System (SLS), Radio Frequency Identification (RFID), Sensors.

***Corresponding author: Email:** devicse17@gmail.com; **Tel.:** +91 9095620265

INTRODUCTION

During the past decades, internet has changed way of the people to communicate with each other by creating a virtual world for both professional and social lives. Internet of Things (IoT) can be considered as an expansion of the internet that will impact our everyday lives and the way we interact with things. IoT can be defined as a world-wide network of interconnected physical things [1]. Smart objectsare the building blocks of IoT, which are things we use every day, enhanced with embedded intelligence as well as connectivity to the internet. A smart object can be a lamp that turns on when you get home, or a TV that knows your favorite shows. Objects that are connected to IoT can communicate using a standard protocol.

The Internet of Things (IoT) is the network of physical objects devices, vehicles, buildings and other embedded devices with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data. [2] When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems which also encompasses technologies such as smart grids, smart cities, industries and homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Researcher estimates that the IoT will consist of almost 50 billion objects by 2020. Internet and its applications have become an integral part of today's human lifestyle.

Smart home is now becoming prevalent with the development of the Internet of things (IoT) techniques. It is aimed at providing the user with a user-friendly method to control the home appliances such as doors, lights, even in a condition of long-distance. This controlling is generally achieved by a mobile phone which can access to the Internet.

REQUIREMENT OF AUTOMATION

When we talked about automated devices which could start with controller, but today it has become a reality.

i) An automated device can replace good amount of human working force, moreover humans are nears to errors and in intensive conditions the probability of error increases where as an automated device can work with usefulness and almost zero error. [3]

ii) Replacing human operators in tasks that involve hard or uninteresting work. Replacing humans in tasks done in dangerous environments (i.e. fire, space, volcanoes, nuclear facilities, underwater, etc)

EXISTING SYSTEM

In this work the detailed study of smart home automation security and privacy techniques are analyzed and studied. Different types of security mechanism are used for access the home control and monitoring. Some technologies are used for authentication purpose like people enter to home means get a notification to the user. The various mechanisms are reviewed in the below section.

In [5] authors A. Jacobsson M. Boldt and B. Carlsson "**A risk analysis of a smart home automation system**" says the surveillance camera can also be used for other personal purposes such as to see who is at home with respect to childcare, control of infants sleeping, elderly care, etc. For example if lamps are switched on or off, doors closed or open, cameras showing water leaks, etc. Smart home surveillance cameras can also be used in combination with other connected devices, which together may provide an overly detailed image of the persons living in that home. In [6] authentication procedures are communicated by cryptography technique and the communication is done between the objects. Based on our research to suggest the following steps should be included in the model:

1. Identification and categorization of the personal data in smart homes.
2. Analysis and description of the main risks to privacy and security.
3. Identification and implementation of preventive, detective measures to shrink risks.
4. Strategy for privacy-friendly information management within smart homes.

The analyzed system was divided into the following six parts [7]
1. Connected sensors/devices/actuators
2. In-house gateway.
3. Cloud server.
4. API (Application Program Interface).
5. Mobile device.
6. Mobile device apps.

In [8] authors Hui Suoa, Jiafu Wana,b, Caifeng Zoua, Jianqi Liua "**Security in the Internet of Things: A Review**" says that the IoT will be faced with more challenges in smart home security system. There are the following reasons:
1) The IoT extends the Internet through the traditional internet, mobile network and sensor network.
2) Every Thing will be connected to this network
3) These Things will communicate with each other.

Day by day new security and privacy problems are identified. In [9] the security issues are to concentrate on confidentiality, authenticity, and integrity of data in the IOT.

Table: 1. Security Algorithms

S.NO	Algorithm	Purpose
1	Advanced Encryption Standard (AES)	Confidentiality
2	Rivest Shamir Adelman (RSA)	Digital signatures key transport
3	Diffie Hellman (DH)	Key agreement
4	Secure Hash Algorithm (SHA)	Integrity

In [10] authors Andreas Jacobsson ,Martin Boldt and Bengt Carlsson "**On the Risk Exposure of Smart Home Automation Systems**" says that smart home automation, energy services depend on a broad range of hardware and software components for monitoring and controlling an apartment or building. The sensors and actuators record the report metrics like water usage, indoor temperature, and power consumption. Each device runs

THE IIOAB JOURNAL ISSN: 0976-3104

independently of each other and communicates using a local mesh network. In this case Zigbee is used with a home gateway and act as the central node. The gateway runs a minimalistic Linux distribution and relays device information to a remote, or cloud, server over the Internet using the protocol.

In [11] the Smart Home Automation System (SHAS) platform used for the connected devices is distributed across multiple hardware solutions, each with its own set of responsibilities and privileges. As the available devices in each apartment differ from each instance of the platform will subsequently be different. The fundamental operations of the platforms are operational capacity the in-house gateway for relaying messages that devices send over the local communication protocol (Zigbee or ZWave) to an Internet-based protocol.

In [12] authors Suvarna Patil, Tanuja Lonhari, Sarika Pati "**Internet of Things: Current Research, Trends and Applications**" says that the term IoT was initially proposed to refer uniquely identifiable interoperable connected objects with Radio Frequency Identification (RFID) technology. After that researchers relate IoT with more technologies such as actuators, sensors, GPS devices, and mobile devices. Today IoT can defined as "a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'Things' have identities, physical attributes, and virtual personalities and use intelligent interfaces are seamlessly integrated into the information network".

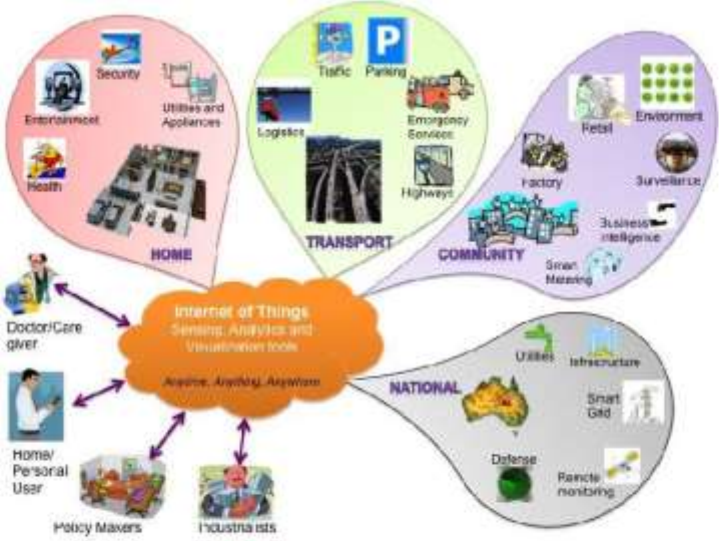


Fig.1: Internet of Things Schematic showing the End users and application areas based on data

Table: 2. A Four Layered Architecture of IoT

S.NO	LAYERS	DESCRIPTION
1	Sensing Layer	This layer is integrated with hardware to sense/control the physical world.
2	Network Layer	This layer provides basic networking support and data transfer over wireless or wired network.
3	Service Layer	This layer creates and manages services. It provides services to

		satisfy user needs.
4	Interface Layer	This layer provides interaction methods to users and other applications.

In [13] authors Sudhir Chitnis, Neha Deshpande, Arvind Shaligram "**An Investigative Study for Smart Home Security: Issues, Challenges and Countermeasures**" says that a home security system to determine the present security status and to find out any extremes of security. It determines the level of protection needed and give suggestions to improve the overall security of home, if required. Traditional techniques of alarm based security have gained much popularity in past decades. Nowadays, embedded system is designed to provide security due to tremendous improvement in microcontroller unit and widespread applications of GSM technology. In [14] most of our homes are still protected by simple lock-and-key mechanisms. Nowadays, most of the families are single type where almost all are working professional. As a result the children at home are left unattended or in the company of servant or a babysitter who are not trustworthy most of the times. Thus, relying on traditional lock-and-key security mechanism is rather risky. Generally, robbery or crimes are committed by low skilled criminals.

In [15] authors Mahnoosh Mehrabani, Srinivas, Benjamin Stern "**Personalized Speech Recognition for Internet of Things**" says that each user was asked to create a set of household devices and select customized names for their appliances. A smartphone application was used by end users as a centralized interface, and speech recognition was performed by connecting to a cloud Application Programming Interface (API). Testers were instructed to issue voice commands including their selected personalized devices. The results presented here are based on a subset of the speech data including 1533 words that was manually transcribed and semantically annotated, and was used as test set. In a smart home scenario each customized devices are connected to home and the user using personalized language model to evaluated the speech recognition.

In [16] authors A. Daramas, S. Pattarakitsophon, K. Eiumtraku1, T. Tantidham N. Tamkittikhun "**HIVE: Home Automation System for Intrusion Detection**" says that the HIVE system deploys three intrusion detection sensors: a passive infrared sensor (PIR), magnetic switch sensor, and load cell sensor. The first sensor, PIR sensor, detects motions in a particular area. The next sensor, magnetic switch, detects the status of doors or windows. There are 2types of magnetic switch: Normally Open (NO) and Normally Close (NC).

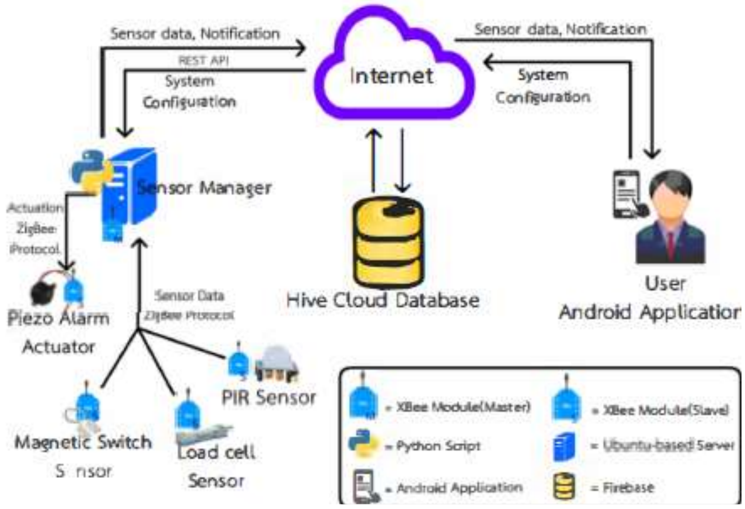


Fig. 2: HIVE System Architecture

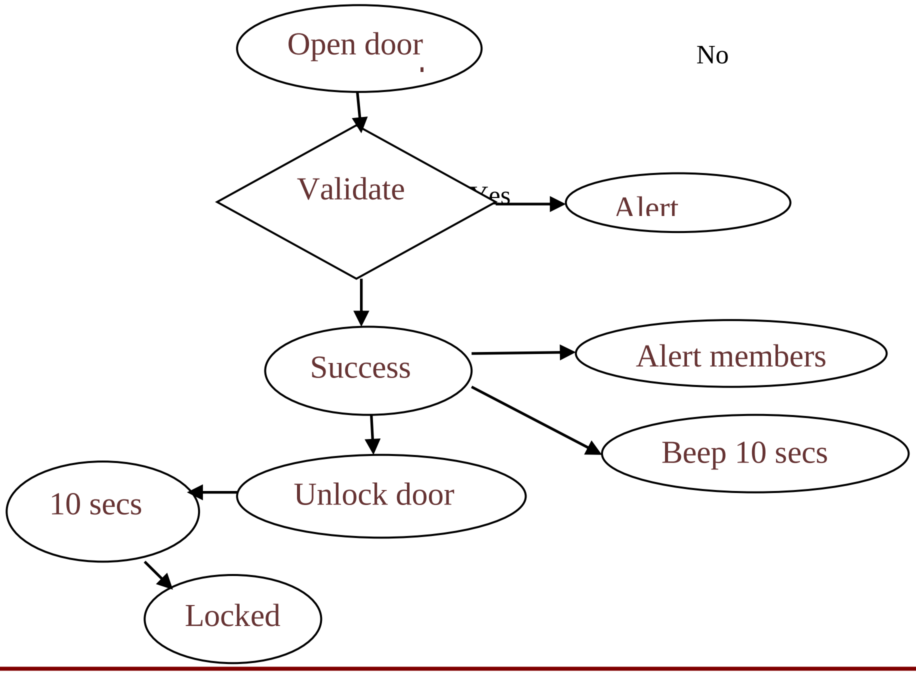
………..

In [17] authors Honglei Ren, You Song, Siyu Yang and Fangling Situ "**Secure Smart Home: A Voiceprint and Internet Based Authentication System for Remote Accessing**" says that a smart home architecture, both in hardware and software. It used the NFC and android technologies to enable remote and local accessing. For the local access, users can enter home by making the mobile phone approach to a NFC reader which can recognize the necessary authentication information. A user Personal Identification Number (PIN) is needed to input on the mobile side for safety considerations. The PIN will be encrypted with other information (like MAC address) to produce a fingerprint of the device, which will be authenticated by the server. In the condition of remote access, the security is guaranteed by the PIN and the Virtual Private Network (VPN) tunnel. The VPN can establish a secure connection without the need of specialized software. However the PIN code can still be hacked without lots of efforts. Human put forward a smart home authentication solution based on fingerprint identification, whereas it is still dangerous when it is defrauded with the fingerprint film.

In [18] authors Abhay Kumar, Neha Tiwar "**Energy Efficient Smart Home Automation System**" says that many smart homes are need security and energy saving. We need to implement and optimize the efficiency of the smart home automation system via simulation. [19] We can also implement the smart home technology using VB (visual basic) is being used. Practically we can implement the smart home by many researchers to optimize the better result and to improve the technology for the less consumption of electricity. We observed the deviation in temperature and the speed of fan and light is also varying according to the temperature as they programmed in coding. And the masses which are connected through relays are used to switch on and switch off the loads through sending tones via mobile phone and through serial connection. We can also control the whole system by connection through PCs with server through client PCs. It will work only with the output voltage of +5V. We feed the coding in PIC microchip to run the system according to the feed coding.

In [21] authors Abdallah Kassem and Sami El MurrGeorges Jamous, Elie Saad and Marybelle Geagea "**A Smart Lock System using Wi-Fi Security**" says that smart-Lock-System is a complete recreation of the standard Key-Door lock .Where all the digital keys are kept in a Digital Keychain kept on the owner's phone. Encrypted and secured Smart-Lock-System can be connected to the Internet through internet cable or Wi-Fi. The Smart-Lock-System consists mainly of three major functions.

Function 1: Door lock controller
Function 2: Central Control
Function 3: Mobile Application



THE IIOAB JOURNAL ISSN: 0976-3104

Fig. 3: Flow Chart for Door Open

……………………………………………………………………………………………………….

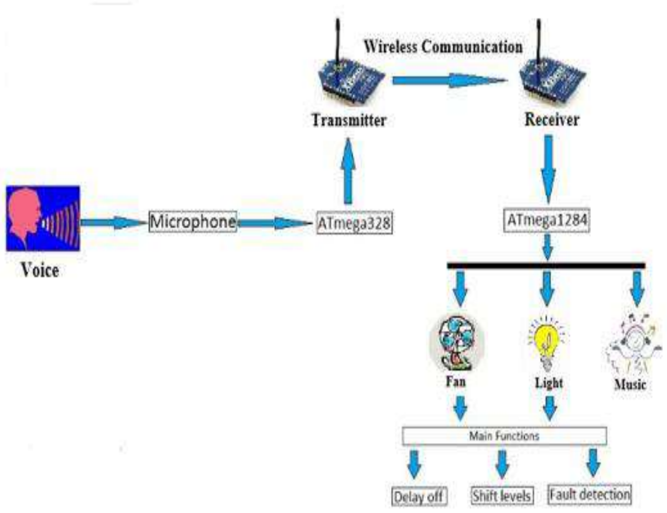


Fig. 2: Overview of logical structure

……………………………………………………………………………………………………….

Existing system having the voice-controlled system is used in smart home automation system. Existing simulation is a product for the future life and the purpose of it is to make people's lives more convenient. The XBee radio module use of a 12V battery for powering the entire device makes it safer one. Similarly, the wireless voice-control system makes it advantageous for disabled people to control the household devices.

COMPARATIVE ANALYSIS OF EXISTING SYSTEM

This section presents the comparison between the different type of algorithm and sensors used and various purposes for controlling home devices. Different types of sensors are used for sensing the data and monitor the movements from home and various sensors and algorithms are reviewed in the comparative analysis section.

COMPARATIVE ANALYSIS

S.NO	Paper Title	Algorithm/Risk/Device	Purposes
1	A risk analysis of a smart home automation system	Home Gateway	To provide authentication
2	Security in the Internet of Things: A Review	AES,RSA,DH,SHA	Confidentiality, Digital signatures key , Key agreement, Integrity
3	On the Risk Exposure of Smart Home Automation Systems	Information Security Risk Analysis (ISRA)	Confidentiality, Integrity availability.
4	Internet of Things: Current Research, Trends and Applications	RFID,GPS	To communicate the system and the user.
5	An Investigative Study for Smart Home Security: Issues, Challenges and Countermeasures	CCTV camera	To capture the video.
6	Personalized Speech Recognition for Internet of Things	Hidden Markov Models (HMM) and Gaussian Mixture Models (GMM)	To represent the time-based variance of speech.
7	HIVE: Home Automation System for Intrusion Detection	Zigbee,PIR sensor,	To detect the movement
8	Secure Smart Home: A Voiceprint	Voice ,Virtual private	To prevent

	and Internet Based Authentication System for Remote Accessing	number(VPN)	unauthorized people to enter
9	Energy Efficient Smart Home Automation System	Light ,Fan ,AC	To reduce the energy
10	A Smart Lock System using Wi-Fi Security	AES ,Key	To provide security

PROPOSED SYSTEM

Overall control of the home is done by smart home automation system using Internet of Things (IOT) In door opening method like Number locking system means user having the pin number to enter the home, the drawback is pin number is misused in other person. The fingerprint system having thumb impression is used to enter the home and the drawback is easy to trace any place. To overcome the number lock and fingerprint system using door locking sensor to capture the face and stored in cloud. Any relations are come to home means to capture the face and send it to the owner. The owner will give the security code and they can enter the home.

CONCLUSION

Our work mainly concentrates on security system in the existing home automation system. Security factor is most important when it comes from automated home security systems. Such system will definitely provide a security to every person at home. And will also to remember their work, that are not present their home. To give a survey on smart home automation many new technologies are exploring day by day. Smart is the good and beneficial one and to save their electrical energy that is wasted by many people in fixed span of time. With the smart home security system the people are living and will obviously live more comfortable life. All the time home can be saved from automation so that we will have much more time work on the other scenario. In this prose we reviewed on smart security mechanism in the IoTand analyzed security characteristics home automation.

CONFLICT OF INTEREST

The authors declare no conflict of interests.

ACKNOWLEDGEMENT

None

FINANCIAL DISCLOSURE

None

REFERENCES

[1] Abdallah Kassem and Sami El MurrGeorges Jamous, ElieSaad and Marybelle Geagea “A Smart Lock System using Wi-Fi Security” 2016 3rd International Conference on Advances in Computational Tools for Engineering Applications (ACTEA).

[2] Abhay Kumar1, Neha Tiwari.[2015]Energy Efficient Smart Home Automation System” International Journal of Scientific Engineering and Research (IJSER) www.ijser.inISSN (Online) 3(1) : 2347-3878

[3] Andreas Jacobsson ,Martin Boldt and BengtCarlsson “On the Risk Exposure of Smart Home Automation Systems” 2014 International Conference on Future Internet of Things and Cloud.

[4] Atzori.L, A. Iera, and G. Morabito, “The internet of things: A survey”, Computer networks, vol. 54, no. 15, pp. 2787–2805, 2015.

[5] Babar S, A Stango, N Prasad, J Sen, R Prasad.[2014] Proposed Embedded Security Framework for Internet of Things (IoT), Int. Conf.on Wireless Communication, Vehicular Technology, Information Theory and Aerospace &Electronics Systems Technology.

[6] Daramas A, S Pattarakitsophon, K Eiumtraku1, T Tantidham. N Tamkittikhun “HIVE: Home Automation System for Intrusion Detection” 2016 Fifth ICT International Student Project Conference (ICT-ISPC).

[7] Gan G, Z. Lu, and J Jiang, “Internet of Things Security Analysis”, IEEE Conf. on Internet Technology and Applications.

[8] HuiSuoa, JiafuWana,b, CaifengZoua, JianqiLiua “Security in the Internet of Things: A Review” 2012 International Conference on Computer Science and Electronics Engineering.

[9] HongleiRen You Song, Siyu Yang and Fangling Situ “Secure Smart Home: A Voiceprint and Internet Based Authentication System for Remote Accessing”.

[10] Jacobsson A , M. Boldtand B. Carlsson "A Risk Analysis on a Smart Home Automation System", Future Generation Computer Systems, Elsevier, 2015. DOI:10.1016/j.future.2015.09.003.

[11] Mantoro.T, MA Ayu, SM. bintiMahmod.[2014]Securing the authentication and message integrity for Smart Home using smart phone", in 2015International Conference on Multimedia Computing and Systems(ICMCS). IEEE, 2014, pp. 985–989.

[12] Mahnoosh Mehrabani, Srinivas, Benjamin Stern "Personalized Speech Recognition for Internet of Things" International Conference on Future Internet of Things and Cloud.

[13] Polkand T., S. Turner. "Security challenges for the internet of things", http://www.iab.org/wp-content/IAB-uploads/2011/03/Turner.pdf

[14] Shi JH, JF Wan, HH Yan, H Suo. A survey of cyber-physical systems", in Proc. of the Int. Conf. on Wireless Communications and Signal Processing, Nanjing, China, November, 2015.

[15] Sudhir Chitnis, NehaDeshpande, ArvindShaligram.[2016] "An Investigative Study for Smart Home Security: Issues, Challenges and Countermeasures" Wireless Sensor Network, 8:61-68.

[16] SuvarnaPatil, TanujaLonhari, SarikaPati.[2015] Internet of Things: Current Research, Trends and Applications" International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) 3(12)

[17] System of Monitoring and Environmental Surveillance, http://www.dimap.es/enviromental-agriculture-services.html (2011). Oxford University Press, ISBN 0-8218-0531-2, 2014.

[18] Yang G, J Xu, W Chen, ZH Qi, HY Wang.[2013] Security characteristic and technology in the internet of things, *Journal of Nanjing University of Posts and Telecommunications (Natural Science*), 30(4).

| Karthika et al. 2016| IIOABJ | Vol. 7 | 6| 1–6