

Survey On IOT Based Optimization Technics For Security Of Health Monitoring System

N.Laxmi
Research Scholar
Department of Electronics and
Communication,
Saveetha school of
Engineering, Chennai, India.

Dr.I.Chandra
Assoc.Prof.
Department of Electronics and
Communication,
Saveetha school of
Engineering, Chennai, India.

Abstract— The Raspberry Pi is a computer with small size compared to our modern computer CPU. the size of it is like our credit card. We can implement a large number of applications in diverse field i.e. Mostly we are using this chip in industry automation & health domain. Raspberry PI is having different communication ports like HDMI port, Ethernet port, USB port, display serial interface, Bluetooth and Bluetooth low energy port. This paper provides survey on combination of Raspberry pi and IOT applications in diverse fields like home automation and health domain and we focus on till now what are the applications developed and what are the challenges faced in security of information transmitted through IOT technology especially in health management applications. The Raspberry Pi is a series of small single-board computers developed in the United Kingdom by the Raspberry Pi Foundation to promote the teaching of basic computer science in schools and in developing countries. We also discuss some of the best projects that have come up so far with the combination of raspberry pi and IOT Technology. The IoT has a much attention from Industry ,research scholars, scientists and government all over the world for its special features in changing modern day living. Primary hypothesis is to have smart sensor dealing directly to deliver a class of applications without any external or human participation. Collection of physical objects that are designed with built in wireless or wired connectivity, so they can be monitored, controlled and linked over the Internet via a mobile app or software that uses with another platform. The recent development of Internet and smartpone and machine-to-machine M2M technologies can be considered first phase of the IoT. In the coming years IoT is expected to be one of the main hub between various technologies by connecting smart physical objects together and allow different applications in support of smart decision making. The security of IoT is becoming important and will take great effects on the industry & health domain. In this paper we

discuss IoT applications, algorithms in various fields and comparing all the algorithms of IOT a and technical aspect that are related to IoT.

Keywords-internet of things (IOT); security of IOT, Raspberry pi, IOT algorithms.

1. INTRODUCTION

The ideas of research scholars and engineers will give new innovations and produce new applications. Before the idea of raspberry pi we worked on Arduino boards. Raspberry pi is a very advanced and cheaper in cost compared to all other boards. There are many applications developed using raspberry pi in diverse fields like industry, home & health automation technologies. Home automation system uses the technology of internet of things (IOT) for monitoring and controlling the electrical and electronic appliances at home from any remote location by simply using a smartphone. The application of ideas, theories, and new innovations is what drives them. , For years the work was done on Arduino boards but with the launch of the very cheap Raspberry Pi it all changed. IOT is versioned as billions of sensors connected to the internet using wireless and other communication technologies. The sensors would generate large amount of data which needs to analyzed, interpreted & utilized. Using IOT and Raspberry pi technology we can implement a low cost and flexible home automation device is presented. In this technology it enhances the use of wireless communication & provides user can control various electrical and electronic appliances using remote.

2. LITERATURE SURVEY ON RASPBERRY PI AND IOT:

Paper 1: Industrial monitoring using IOT:In this paper the author Dinesh Kumar implemented industrial monitoring device using IOT. In this system sensors like temperature sensor, humidity sensor are used and data collected from this sensors will be available remotely through web pages and can view the data anywhere in the world and decisions will be taken based on the measurement. In this paper author did not concentrated on the security of the transmitted data from sensors through web pages. In wireless communication the others can view our data and they can modify it. So we may get big problem. So in my paper we are much focusing on the IOT security algorithms.

Paper 2: Health monitoring system using IOT and raspberry pi- a review: Vivek Pradesh Dept. of Ext Egg. Space, wardha, MH, India. In this paper also author proposed a health monitoring system using IOT. In this paper also he did not take care about the security of the data transmitted through wireless network. If data/information transmitted wirelessly others can attacks our data and misuse it or modify it and transmitted to the doctor wirelessly and he may monitor patient according to the data which he got from the internet. So to avoid this type of problems we use IOT security algorithms for reliable operations.

Paper 3: Security of internet of things: perspectives & challenges: Qi Jing. Athanosi:-In this paper author focused on security architecture of IOT, which divide IOT into layers and sub layers, and explained about major technical supports of each sub layer and proposed security architecture to the problems of these technologies. In this paper they analyzed cross-layer heterogeneous integration issues & security issues in details. We took this paper as our reference for our problem and we analyze the security issues facing in wireless networking transmission In IOT there are two major security issues in transmission process they are-(1) IOT security is from itself(2) Other one is from the related technology of construction and implementation of the network functions.

IOT is the integration of multiple heterogeneous networks, it should deal with compatibility issues between different networks

Basically security issues are: DOS/DDOS attacks, forgery/middle attacks and Heterogeneous network attacks, application risk of IPv6, WLAN application conflicts also affect the transport security of IOT.

Basically IOT consist of three layers:-

- Perception layer
- Transportation layer
- Application layer

In this paper we are focusing the security problems facing in transportation layer & solving the problems using specific IOT algorithm. The main issues of Transportation layer are :(1) Heterogeneous network coverage issues (2) Transportation layer attacks issues. The transportation layer of IOT is vulnerable to Trojan horses, viruses, spam & other attacks will lead to information disclosure and network paralysis. In this layer we mainly focus on security issues for the access network, here we analyzed security issues for WIFI and 3G network and provides corresponding solution. In transportation layer we focus on

- Access network
- Core network
- Local area network

In core network we analyze the security of massive number of nodes and introduced 6LowPAN i.e. one of the IOT algorithm.

3. TYPES OF RASPBERRY PI

Raspberry Pi is a series of credit card size single computer board developed by raspberry pi foundation in the United Kingdom. They develop free resources to help people to learn about computing and how to make applications with computers. Raspberry pi began in 2006 but finally released in 19th February 2012 with two models are model A and model B. Raspberry pi is a low cost minicomputer connected to many devices like sensors, mouse and keyboard for different applications and it is having their own OS on Raspberry PI SD cards. After the sale of 3 million units in May 2014, the latest Model B+ was announced in July 2014. Raspberry Pi board costs only \$35 and does the work of a computer costing hundreds of dollars. Though its purpose is not to replace computers, laptops etc. but to work supplement with them. Boot it up, and you have a got a fully functional powerhouse. Put four-gigabyte SD card and

flash it with the free Linux-based operating system on the Raspberry Pi Foundation's website. Put the SD card into the slot, apply power, and you've got a 700 megahertz workstation with hardware accelerated 3D graphics. The Raspberry Pi offers another path: encouraging experimentation by lowering the cost of accidentally breaking when you're trying to be making. The computer was conceived of by Eben Upton, formerly a lecturer at the University of Cambridge, U.K., who created the Raspberry Pi Foundation to make it a real product. Upton is also a veteran of several years at chip maker Broadcom, designing the kind of chips that make it possible to sell a complete computer for \$35. Now a days IOT is becoming an established part of life by extending the communication and anywhere .so security becomes more important in IOT technology. This paper gives the detailed survey and analysis of IOT security algorithms especially in the area of health domain. IOT will consist of billions of digital devices and people and other physical objects this will make our lives simpler through digital environment. Security for IOT will be a critical concern due to manifold aspects involves must be addressed in order to enable several current and future applications. Hence providing privacy and safety are the essential features of IOT this security is related to tag information (RFID), wireless communication information, network security of information. Therefore it is necessary to have through research on design and improvement of security in IOT. Technical Specifications of Raspberry and The following are specifications for Model B+:

- Broadcom BCM2835 Sock processor with 700MHz ARM1176JZF-S core
- 512MB RAM
- Video core 4 GPU supports up to 1920x1200 resolution
- Micros card slot
- 10/100Mbps Ethernet port
- 4 x USB 2.0 ports
- HDMI, audio/video jack
- GPIO header containing 40 pins
- Microbus power port providing 2A current supply
- DSI and CSI ports
- Dimensions: 85.6x56mm

The software's offered are RASPBIAN, PIDORA, OPENELEC, RASPBMC, RISC OS, and ARCH LINUX. All these software's can be downloaded easily and for free from the official forum under slipped in easily. Note that the Raspberry Pi have their OS on SD cards that can be removed and replaced to replace the entire operating system. You can get more information on the Raspberry Pi website.

Advantages of Different Raspberry Pi Models

- The size of the raspberry pi is in small of credit card
- The price of the raspberry pi is low
- Gathering a set of raspberry pi to work as a server is more effective than the normal server.
- Applications of Raspberry pi
- The different applications of the raspberry pi model are
- Media steamer
- Tablet computer
- Home automation
- Internet radio
- Controlling robots
- Cosmic Computer
- Arcade machines
- Raspberry pi based project

Comparison of Raspberry pi models :

	Raspberry Pi 1 Model A	Raspberry Pi 1 Model A+	Raspberry Pi 1 Model B	Raspberry Pi 1 Model B+	Raspberry Pi 2 Model B	Raspberry Pi 3 Model B	Raspberry Pi Zero
USB 2.0 Ports	1	1	2	4	4	4	1 (Micro-USB)
Ethernet	None	None	10/100 Mbit/s	10/100 Mbit/s	10/100 Mbit/s	10/100 Mbit/s	None
Bluetooth	None	None	None	None	None	4.1	None
WiFi	None	None	None	None	None	802.11n	None
Audio In	I ² S	I ² S	I ² S	I ² S	I ² S	I ² S	I ² S
Audio Out	I ² S, analog (3.5mm jack), digital (HDMI)	I ² S, analog (3.5mm jack), digital (HDMI)	I ² S, analog (3.5mm jack), digital (HDMI)	I ² S, analog (3.5mm jack), digital (HDMI)	I ² S, analog (3.5mm jack), digital (HDMI)	I ² S, analog (3.5mm jack), digital (HDMI)	Digital (mini-HDMI), analog GPIO PWM
Video In	CSI Camera Connector	CSI Camera Connector	CSI Camera Connector	CSI Camera Connector	CSI Camera Connector	CSI Camera Connector	None
Video Out	HDMI, Composite (RCA)	HDMI, Composite (TRRS)	HDMI, Composite (RCA)	HDMI, Composite (TRRS)	HDMI, Composite (TRRS)	HDMI, Composite (TRRS)	Mini-HDMI, GPIO Composite
External Storage	SD	MicroSD	SD	MicroSD	MicroSD	MicroSD	MicroSD

Fig: Different Raspberry pi models

4. IOT PROTOCOLS:

In this paper we summarize and differentiate

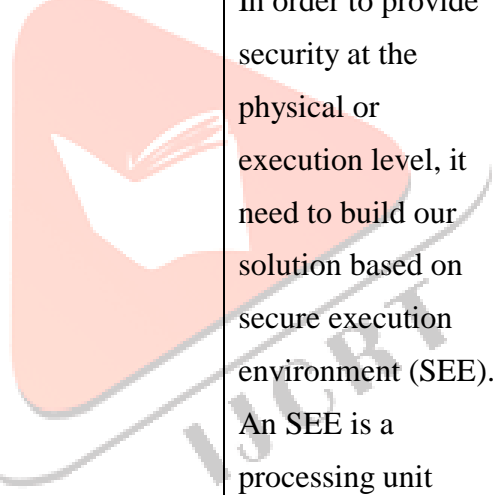
Five IOT protocols:-

- An IPsec -based security (internet protocol security)
- Wireless HART
- 3.6LoWPAN
- IEEE802.15.4
- Embedded security

Wireless HART: It is a protocol and provides several layers protection. All traffic is secured, the payload is encrypted and all messages are authenticated. Wireless HART requires all devices are provisioned with a secret join key as well as a network id in order to join the network. A set of different security keys are used to ensure secure communication. A new device is provisioned with a join key before it attempts to join the wireless network. The join key is used authenticate the device for a specific wireless HART network.

6LoWPAN security requirements: The RFC 4919, specifies a list of security requirements for 6LoWPAN, which mainly aim at protecting the communication from the end user to sensor network. IT provides high security by using cryptography for 6LoWPAN. Cryptography alone cannot provide total security for 6LoWPAN. There is need for implementing IDS to monitor any malicious behavior of the network to prevent early security attacks to decrease its effects. The combination of cryptography and IDS defense can secure the network from most of the threats. This algorithm provides more security than other algorithms.

WirelessHart	6LoWPAN IEEE	802.15.4	IPSec	Embedded Security
bidirectional network of relatively powerful devices and has a central network manager and controller as of version 7, HART also incorporates an IEEE 802.15.4-based wireless mesh network as an option for	Per-hop security with at least integrity protection should be used in 6LoWPAN networks to prevent unauthorized access through the radio medium, and to defend against effortless	for message authentication and encryption on a per-hop base in 6LoWPAN networks	The most known algorithms are MD5 and SHA. In addition, Non repudiation, availability and authenticity are guaranteed by communication protocols like IPSec for example.	The hash of information is used to check the integrity of a message by providing a signature which is unique for each message. The most known algorithms are MD5 and SHA

the physical layer.	attacks launched to waste constrained resources.			
Wireless HART Security Manager	Cryptography techniques Intrusion detection system techniques	protects a communication on a per-hop base where every node in the communication path has to be trusted. A single pre-shared key is used to protect all communication.		multiple independent processor cores, secondary bus masters such as DMA engines, and large numbers of memory and peripheral bus slaves.
	IDS protection layers	Roman et al proposed key management systems for sensor network in the context of the IoT that are applicable to link-layer security.		In order to provide security at the physical or execution level, it need to build our solution based on secure execution environment (SEE). An SEE is a processing unit which is capable of executing applications in a protected manner, meaning the attacks originating from outside the SEE cannot tamper with code and data belonging to the SEE. The first building block of an SEE is of course

			<p>a secure processor – either a dedicated processor or one capable of supporting a secure mode, which is hardware compartmentalized from the non secure mode. Utilizing a dedicated processor has the advantage of ease of separation as well as offloading the main processor from handling security tasks. The disadvantage of a dedicated processor is the increase in silicon footprint</p>
--	--	--	---

Table : Security Technique Used

Current Internet security protocols are well-known and widely trusted suite of cryptographic algorithms:

- The Advanced Encryption Standard (AES) block cipher for confidentiality;
- The Rivets-Shamir- 9Adelman (RSA) asymmetric algorithm for digital signatures and key transport;
- The Daffier-Hellman (DH) asymmetric key agreement algorithm;
- The SHA- 1 and SHA-256 secure hash algorithms.

This suite of algorithms is supplemented by a set of emerging asymmetric algorithms, known as Elliptic Curve Cryptography (ECC):-As reported by Anna Johansson at Technology Tell, control, who provides the software plumbing for some of the largest home security vendors, recently published a study on the Smart home. The results were conclusive regarding home security: 90% of respondent’s ranked home security is one of the most important elements of the Smart home.67% ranked home security as the most important element.100% said that they wouldn’t install a Smart home system if it didn’t include home security. The Internet of Things Consists Of Three Main Components: 1. the things (or assets) themselves.2. The communication networks connecting them.3. The computing systems that make use of the data flowing to and from our things Characteristics of IOT: Pervasive (Ubiquitous)

(Embedded everywhere). Heterogeneous (Many technologies interact each other) Scalability (Order of magnitude higher than current internet). The tables as shown below summarize and differentiate five IoT protocols in term of security goals, security threats security, and technique used and design challenges. There are three ways enterprises can manages Internet of Things using modern techniques. Use automated methods for organizing and retaining data based on the content. Securely consolidate IoT data regardless of where it came from or where it's kept Offer new ways to access information, be productive and add value. In this paper, conducted survey and discussed that many new technologies and applications and drawbacks have been overcome for IoT.

Advantages

- Lower operating costs
- Efficiency and lower operating expenses
- remotely control your world!
- providing accurate data
- Decision making
- INTRICATE TECHNOLOGIES
- Various technologies are involves implementing the idea of IOT. In this paper we will focus on these.

- Radio frequency Identification (RFID)
- Near Field Communication (NFC)
- Machine-to-Machine Communication (M2M)
- Vehicle-to-Vehicle Communication (V2V)

IOT Security Issues and Requirements: "According to "Hue Sula" Security features Perceptual nodes (sensors) are short of computer power and limited storage capacity so unable to apply frequency hopping communication and public key encryption algorithm to security protection Security requirements Use lightweight encryption technology becomes important, which includes Lightweight cryptographic algorithm. Issues according to "Kai Zhao" Sensor nodes have many varieties and high heterogeneity. Several Common Kinds of Attack are:

- Node Capture
- Fake Node and Malicious Data
- Denial of Service Attack
- Timing Attack
- Routing Threat
- Replay Attack
- SCA (Side Channel Attack)

Issues according to "Weise Zhang", Physical capture: Many nodes are statically deployed in the area and can easily be captured by attackers and thus, are physically risky. Brute force attack: limited ability of resource storage in sensor node is the big issue to hack by brute force attack. The attacker utilize his encryption algorithm experience in decode the encoded files and messages. Clone node: Attacker can

easily copy the node because hardware structure of several perceptual nodes is simple. Impersonation: Authentication in the distributed environment is very difficult for the perceptual node, allowing for malicious nodes to use a fake identity for malicious or collusion attacks routing attack: Intermediate nodes may be attacked during data forwarding and relay through nodes.

Denial of service (Do's) attack: Nodes can easily be trapped under Do's attack, Node privacy leak: The attacker can passively or actively steal sensitive information in the node.

Applications: Applications of IoT are very diversify. Applications of IoT are increasing every day in many domains. Every day individual /industrial changes our needs and as per need we use the Internet and hence Internet-of-Things. There are plenty of applications of IOT. In coming years, IOT will be more revolutionized because of the RFID, NFC, M2M and V2V communications. By implementing IoT in retail chain monitoring has many advantages: RFIC and NFIC can be used to monitor every detail such as commodity details, purchasing of raw materials, production and sales of product after sale service. With the help of IoT, one can track the inventory in the warehouse so that one can have information about stock, customer's satisfaction etc. and result in increased sales. The system can report pipe flow measurement data regularly, as well as send automatic alerts if water use is outside of an estimated normal range. This allows a smart city to determine the location of leaking pipes and prioritize repairs based on the amount of water loss that could be prevented

Smart homes and offices. In recent time, human life is surrounded by thousands of electronic gadgets like microwave ovens, refrigerators, heaters, air conditioners, fan and lights. By installing actuators and sensors will assist to utilize the energy sufficiently and add comfort in life. These sensors will measure the outside temperature and even can determine the occupants inside the rooms and thereby control the amount of heating, cooling and flow of light etc. This practice would result in minimizing the cost and increase energy saving. M2M and V2V Communication Domain. Industrial maintenance: It is necessary to monitor the temperature and vibrations of industrial motors and to detect the irregular operation in it. The sensors installed on these machines will keep industrial maintenance, by keeping the equipment running efficiently in a factory, cleaning, lubrication and repairs. This preventive maintenance is typically a vital part of industrial field. Companies waste billions due to inefficient maintenance management. This will help Companies to save money and time. Smart cars: M2M communication and smart cars is a best way to minimize accidents. A pilot to operate remote control car in order to minimize car accident and reduce human error was developed by McGill University [24]. These driverless cars will provide functioning more than just safety such as they can save valuable time, reduce stress of driving etc. Some studies carried out by the Institute of Electrical and Electronics Engineers (IEEE) reveal that, by 2040, driverless cars will account for up to 75 percent of cars on the road worldwide.

Smart grid : Smart grid is an electrical grid, which is designed to NFC has created a great ease in travelling; it can to minimize different checks at restaurants. For instance if a person book a room in hotel, a secret digital key would be provided to that person. By using that secret digital ticket, with NFC enable lock, a person can go to booked room without wasting time in lounges.

Health: NFC also plays a great role in monitoring personal health. It has information and data about health of patient and sends it to health monitoring center. By analyzing this data at health center, valuable information is provided to individual.

5. CONCLUSION

World has been changed completely due to Internet and Internet based application development. Interaction in all scenario becomes seems impossible without it. IoT has potential to broaden its horizon by enabling communication between smart objects. IoT will changed everything drastically if implemented successfully, But still there are various issues which need thorough research to improve the quality of life. In this Paper, we have discussed various technologies with its specification that can result in making IoT a reality. In next section, we presented some handsome application of IoT and its comfort in life. Finally, some important issues that needed to be resolved have been discussed before wide acceptance of this technology. We finally conclude the need for new “smart” autonomic management, data aggregation, and protocol adaptation services to accomplish better integration among IoT service.

REFERENCES

- [1] “Industrial monitoring using IOT” by p.dinesh kumar IJIRCCE ,Vol.5,Issue 3,March2017.
- [2] K. Navy, Dr. M. B. R. Murthy, “A Zig bee Based Patient Health Monitoring System”, Int. Journal of Engineering Research and Applications Vol. 3, Issue 5, Sep-Oct 2013, pp.483-4862.
- [3] A Technical Seminar on “A Survey in Privacy & Security in Internet of Things” by sultan baseman.
- [4] Improving the Security of Internet of Things Using Encryption Algorithms International Journal of Computer and Information Engineering, Vol: 11, No: 5, 2017.
- [5] Bruce D, GR. Milne, Y.G.Andonova, and F M Hajj at “Internet of Things: Convenience vs. Privacy and secrecy “Business Horizons 58, no.6, science Direct, pp.615-624, 2015.
- [6] Tsai, c., Laic. & vasilakos,v.(2014)Future internet of things:open issues and challenges.ACM/Springer wireless Networks,doi:10.1007/s11276-014-0731-0.
- [7] International Telecommunication Union (2005). Internet Reports 2005: The internet of things. Geneva: ITU.
- [8] Nakul Padhye and Preeti Jain, “Implementation of ARM Embedded Web Server for DAS using Raspberry pi”, VSRD IJEECE April 2013.
- [9] Ch. Sandeep Kumar Subudhi and S. Sivanandam, “Intelligent Wireless Patient Monitoring and Tracking System (Using Sensor Network and Wireless Communication)”, International Journal of Interdisciplinary and Multidisciplinary Studies, 2014, Vol 1, No.3, 97-104.
- [10] Hossein Fotouhi, Aida Causevic, Kristina lundqvist , Mats bjorkman,” Communication and Security in Health monitoring System – A.Review”, 2016 IEEE 40th Annual computer software and application conference, DOI 10.1109/COMPSAC.2016.8
- [11] M. U. Ahmed, M. Bjorkman, and A. Cauševic, et al. An overview on the internet of things for health monitoring systems. In IoT Technologies for HealthCare, 2015.
- [12] F. Samie and L. Bauer and C.-M. Hsieh et al. Online binding of plications to multiple clock domains in shared fpga based systems. InDATE, pp. 25–30, 2015.C. Pereira and A. Zaslavsky and P. Christen et al. Context aware computing for the Internet of Things: A survey. IEEE Communications Surveys & Tutorials, 16(1):414–454, 2014.
- [13] FaradSame, Lars Bauer, Jorge Henkel, “IoT Technologies for Embedded Computing: A Survey”. International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2017).
- [14] Han, J., Choi, C., Park, W., Lee, I. and Kim, S. (2014) Smart Home Energy Management System Including Renewable Energy Based on Zig Bee. IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, 10-13 January 2014, 544-54.

- [15] Jaradat, M., Jar rah, M., Jararweh, Y., Al-Ayyoub, M. and Bousselham, A. (2014) Integration of Renewable Energy in Demand- Side Management for Home Appliances. International Renewable and Sustainable Energy
- [16] Conrera and A. Zaslavsky and P. Christen et al. Context aware computing for the Internet of Things: A survey. IEEE CommunicationsSurveys & Tutorials, 16(1):414–454, 2014.

