IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

A Survey on Challenges, Technologies and Applications of IoT

M.Suruthi[1], **D.Nivetha**[2]

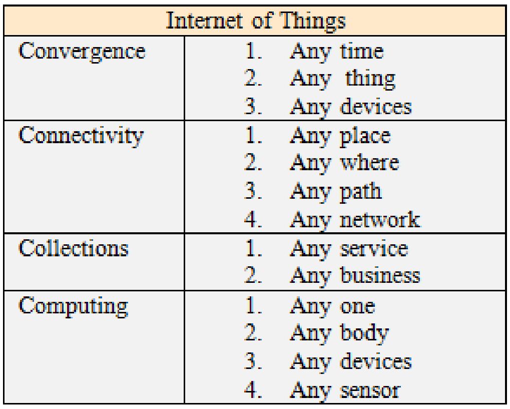
PG Scholar, Department of CSE, Valliammai Engineering College, Kancheepuram, India [1,2]

Abstract: This paper presents IOT (internet of things), which compromises capabilities to detect and connect worldwide physical object into an integrated system. As a measure of internet of things serious concerns are elevated over access of individual privacy and personal data pertaining device .This survey summaries the elements, challenges, evolution, application, security and privacy concerns of internet of things.

Keywords: Internet of Things, Privacy and Security, Sensors

I. INTRODUCTION

With the quick development of communication technology and internet technology, survives are progressively led into unreal space of virtual world. People can shop, chat, work, keeps plants and pets in the virtual would provide by the network. Though, human being lives in an actual world, human action cannot be entirely applied through the services in the imaginary space. It is the restraint of imaginary space that restricts the development of internet to give better services. To eliminate these constraints, a technology is essential to integrate real world on a same platform and imaginary space. Based on a maximum number of low-cost wireless communication sensors, the sensor networks forward new demands to the internet technology. It will carry changes to the upcoming society; change our business model and way of life.



Internet of Things	
Convergence	1. Any time 2. Any thing 3. Any devices
Connectivity	1. Any place 2. Any where 3. Any path 4. Any network
Collections	1. Any service 2. Any business
Computing	1. Any one 2. Any body 3. Any devices 4. Any sensor

Table.1 Internet of Things

II. OVERVIEW AND BACKGROUND

A. *Internet of Things*

The internet of things permit things and people to be connected anyplace, anytime, with anyone and anything perfectly using any network/path and any service [1,21]. They are material objects connected to material objects in the internet. For illustration, through laser scanners, RFID, infrared sensors, global writing system and further information sensing devices are connected to several object for data exchange and communication services. At last, to reach the smart devices to be tracked, monitored and to handle the network functions and to located, to make the physical infrastructure and IT infrastructure consolidation internet of things is the most needed one [21].

Fig.1 Internet of Things Example

III. ELEMENTS

A. *Radio Frequency Identification*

This technology is used in embedded statement, for planning of microchips for wireless data communication [23].

B. *Wireless Sensor Networks*

These are low cost, efficient, low power devices useful in remote sensing applications [23].

C. *Addressing Schemes*

Addressing schemes are useful to individually identify the things. i.e. smart objects [23].

D. *Data Storage and Analytics*

It agreed with storing and sharing of large amount of data. The data have to be stored and used intelligently for actuation and smart monitoring [23].

IV. CHALLENGES

Major challenges while IOT involves:

A. *Scalability*

One more main challenge is the scalability of the internet of things, as daily new devices and objects are getting

DOI 10.17148/IJARCCE.2016.53169

connected with the network. It includes issues like naming and addressing conventions, service management and information management etc [23].

B. Device Heterogeneity

As internet of things is almost connecting several smart devices, connecting heterogeneous devices is main challenge while building internet of things. Such device runs on dissimilar platforms, they usages different protocols to communicate. So it is essential to do unification of such devices [23].

C. Energy Optimized Solution

This is main constraint of internet of things. As numerous devices are connected via networks, energy spent for data communication between different devices [23].

D. Ubiquitous Data Exchange Through Wireless Technology

In internet of things, wireless technologies are used to connect smart devices. Include issues like network delays, congestion and availability etc [23].

E. Self-Organization Capabilities

In internet of things, it is necessary that the smart objects should sense the environment and autonomously respond to real world situations, without abundant human intervention [23].

F. Localization and Tracking Capabilities

The smart objects required be tracking and identified of them is necessary [23].

G. Semantic Interoperability and Data Management

Internet of things interchange data between different smart objects, it is essential that there should be a standardized format for data exchange in order to make sure the interoperability among applications [23].

CHALLENGES	
Challenges in sensing and communication technology	Standardization Interoperability Noisy data Massive data issue Scalability
Challenges in communication protocol	Power consumption Special gateway REQUIRED Security challenge in 6LowPAN Routing
Challenges in middleware	Standardization Abstraction Scalability Heterogeneity and zero infrastructure
Challenges in QOS	Resource constraints Dynamic infrastructure Scalability Heterogeneous Traffic

Table.2 Open Challenges in Internet of Things

V. EVOLUTION

Earlier the investigation of the internet of things in depth, it is valuable to look at the evolution of the internet. In the late 1960s, communication among two computers was made possible through a computer network. In the initial 1980s, the TCP and IP stack was introduced. Then, commercial use of the internet started in the late 1980s. Late, the world wide web because presented in 1991 which made the internet extra popular and stimulate the rapid growth. Then, mobile devices connected to the internet and formed the mobile internet. With the appearance of social networking, users taking place to become connected organized over the internet. The next step in the internet of things is where objects around us will be capable to connect to each other and communicate via the internet. What we want, and what we need and act accordingly without explicit instructions [1,21].

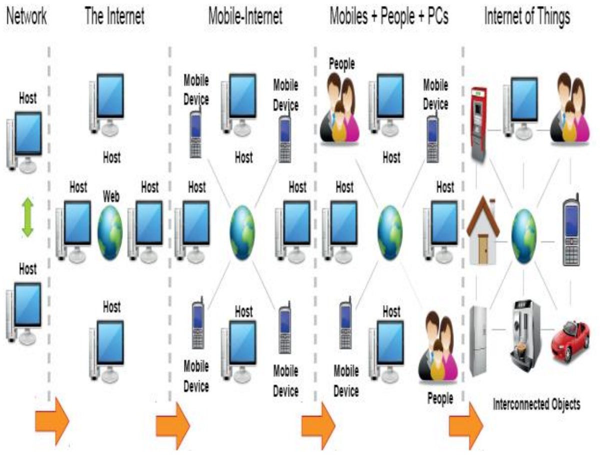


Fig.2 Evolution of the Internet of Things

VI. EMPOWERING TECHNOLOGIES

A. Communication and Sensing Technology

i. Radio Frequency Identification

It is a technology which electronically records the presence of an object using radio signals. Radio frequency identification system is collected of one or more radio frequency identification reader and radio frequency identification tags. Each RFTD (radio frequency identification) has its sole identification number. Radio frequency identification readers, query to radio frequency identification tag by triggering it with suitable signals. Radio frequency identification tag is response sends its tab unique identification number [2,22]. There is passive radio frequency identification which harvests the power from incoming signals from radio frequency identification readers. Active radio frequency identification has own battery power and can instantiate the communication. Merits of radio frequency identification is that it is of very low cost, small in size and can be operated without line of sight, but at the similar time, the biggest demerits is that it has limited battery power.

ii. Wireless Sensor Networks

It contains of large number of spatially distributed intelligent sensor nodes, having the capabilities of processing, analysing, collecting the raw data and can issue the processed information. Wireless sensor networks can be verified better as compared to radio frequency identification while tracking the moving object, as it traces location along with its surrounding atmosphere parameter like temperature and humidity etc. Most of the wireless sensor networks can be applied through various IEEE 802.15.4 standard wireless technologies; Wireless local area network, Wireless personal area network, Wireless metropolitan area network, Satellite network and Wireless wide area network [1,22]. Wireless sensor networks works on two major types of protocol such as IP-based protocols (PhyNet, NanoStack and IPv6) and non-IP based (Sensor-Net and Zigbee). The best part of wireless sensor networks is that it has high radio coverage range so no special device like radio frequency identification is required.

iii. Two Dimensional Barcode

It is a technology which uses optical resources for representing data that can be read by a special bar code reader machine to achieve the data. It shelters several inches to few feet distance but bar code and reader should be in line of site. The tear and wear is more in two dimension code as compares to radio frequency identification but at the similar time it is low-cost technology compare to radio frequency identification [3,22].

B. *Middleware*

Middleware is a software layer which offer abstraction by interfacing underlying technologies of internet of things and its application level. It permits the application running through multiple platforms that hides the heterogeneity, location of sensing devices and delivers interoperability between the heterogeneous devices [4,22].

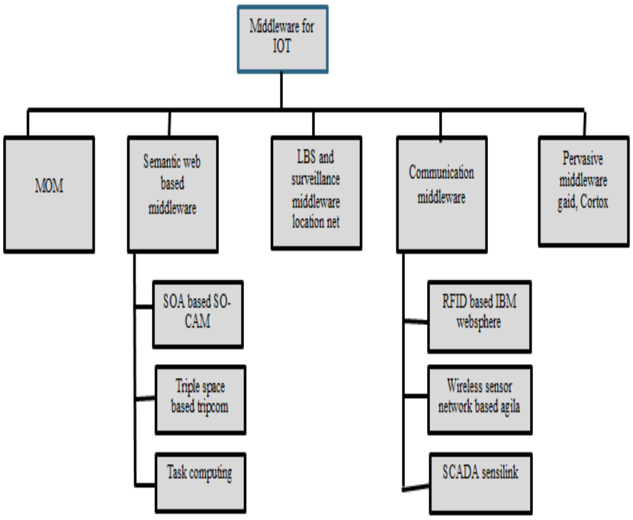

Middleware for IOT
MOM
Semantic web based middleware
LBS and surveillance middleware location net
Communication middleware
Pervasive middleware gaid, Cortox
SOA based SO-CAM
Triple space based tripcom
Task computing
RFID based IBM websphere
Wireless sensor network based agila
SCADA sensilink

Fig.3 Classification of Middleware

C. *Protocols*

Internet of things essentials various protocol for diverse operations. Like it involves a protocol for collecting the information from sensors, communication protocol to send the data to server infrastructure, protocols for device to people communication, protocol for D2D and M2M communication [5,22].

- Message queue telemetry transport MQTT [5,6]
- Constrained application protocols-COAP [5,11]
- Extensible messaging and presence protocol-XMPP [5,6]
- Data distribution service–DDS [5,6]
- Zigbee [7,8]
- Zwave[7,8]
- 6LowPAN[9,10]

VII. APPLICATIONS

A. *Internet of Things in Smart Home*

At the present, smart homes are becoming additional cost effective and intellectualized with continued progress and cost decrease in communication technology, electronics and information technology, which connects the internet with sensor and normal devices for connecting physical and virtual objects through the data capture and communication capabilities development[21]. Reading of remote meters can be achieved through these smart home systems. That indicates, the data linked with home power, gas, water and telecommunication can be sent automatically to their corresponding value company to improve the efficiency of the work. In adding, by virtue of smart home system, home ventilation, windows, lighting, doors, air conditioning etc., can be controlled remotely. Every electronics devices such as washing machine, refrigerator and oven etc., can be manipulated by remote program or platforms. Entertainment equipment like television and radio can be connected to common channels which are in remote. In adding healthcare and home security are also significant aspects of smart homes. For example, health aid devices can help an elder single to send alarm or request to a professional medical center or a family member. In smart home design the home and various electronic appliances have been prepared with sensors and actuator [21].

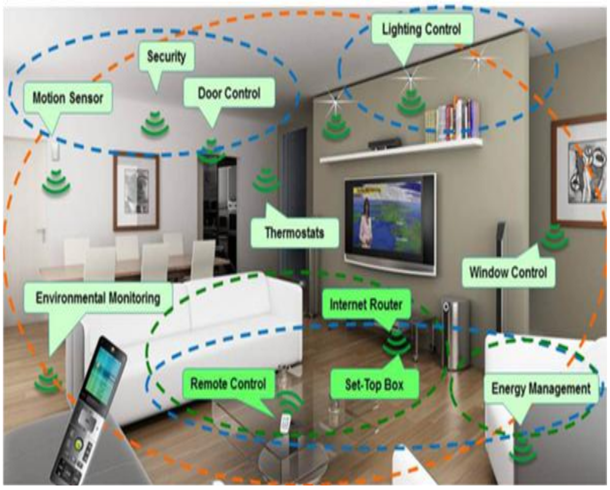


Fig.4 Internet of Things Smart Home

B. *Internet of Things in Health Care*

The internet of things technologies such as radio frequency identification, wireless sensor networks etc., could deliver various benefits in the healthcare domain. For illustration, a person heath status could be inferred from the radio frequency identification tags on clothes or from discovering wearable medical devices. And the application can be categorized in to tracking of patients and hospital staff, authentication and identification of people, remote healthcare and automatic data sensing and collection [12,13].

DOI 10.17148/IJARCCE.2016.53169

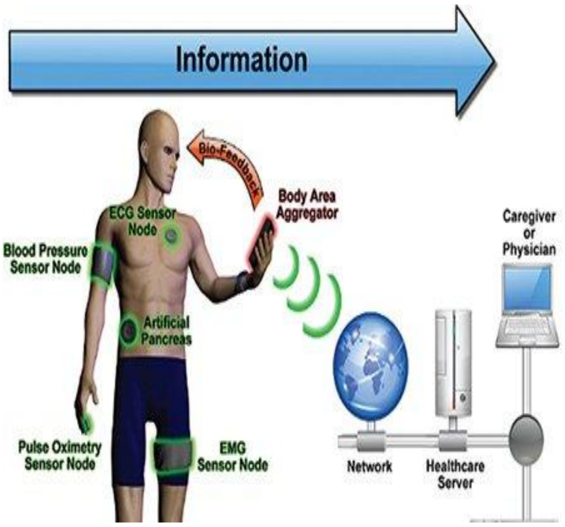


Fig.5 Internet of Things in Healthcare

In the remote health system [13], each day blood glucose level, human blood oxygen concentration are collected automatically by the sensor nodes, transmitted wirelessly to the base station and displayed compared to time on the screen [13]. Moreover by connecting the base station with a networked home person computer, doctors may check the data to see if the results are normal or not. The data can be transferred to doctor mobile devices through the gsm short message from the home base station. This system gives benefits to hospital or remote healthcare at homes.

C. *Intelligent Community Security System*

The ICSS (intelligent community security system) embraces various subsystems, such as surrounding security subsystem (SSS), vehicle management subsystem (VMS), property management subsystem (PMS), central information processing system (CIPS) and fire and theft prevention subsystem (FIPS) [14]etc.

i. Vehicle Management Subsystem

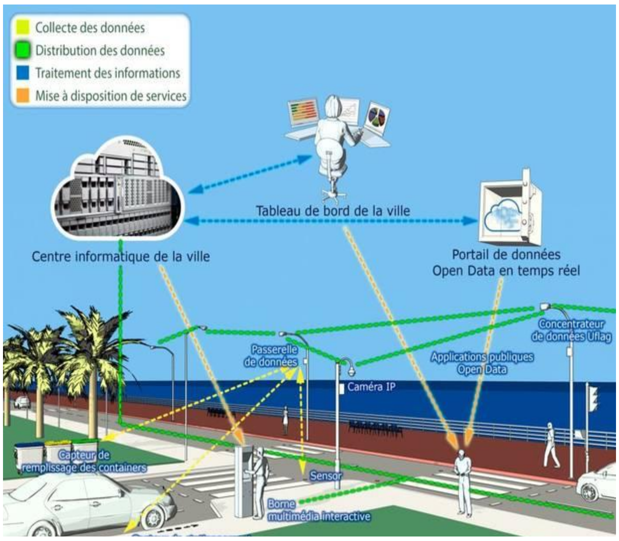

Collecte des données
Distribution des données
Traitement des informations
Mise à disposition de services
Tableau de bord de la ville
Centre informatique de la ville
Portail de données
Open Data en temps réel
Concentrateur de données Urlag
Passerelle de données
Applications publiques Open Data
Caméra IP
Capteur de remplissage des containers
Sensor
Borne multimédia interactive

Fig.6 Vehicle Management System

The VMS [14] in intelligent community security system accepts intellectual property rights, radio frequency identification and sensor network technologies. Image registration can be taken by video camera and radio frequency identification which is given to the vehicle. The vehicle license data will be messaged to the central information processing system, when enter the communities.

The visitor is assigned with the short-term parking places. The record information and the data of the driver radio frequency identification card must be coherent when the car leaves. This assurance the security of the car and prevents theft occurrences. In the garages video system will check damage or stealing to assure the vehicle security.

ii. Surrounding Security Subsystem

As per the essentials of security surroundings to create an intelligent and enclosed community, sensing terminals such as Unicode infrared laser, power network and sensor optical fibre rare installed. WSN collect the valuable feedback and information to the central information processing system at regular time intervals [14]. The surrounding security subsystem surrounds electronic access controls electronic fences and rotatable watching cameras. It can be applied to escape illegal intrusive behaviour or enter in to communities.

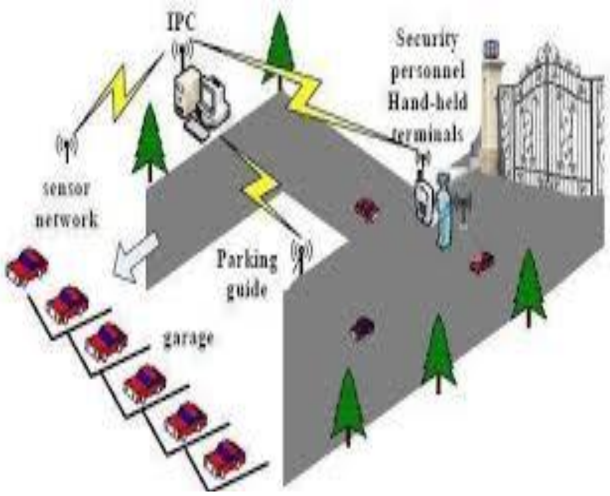


Fig.7 Surrounding Security Subsystem

The subsystem can catch the correct location of the accident by utilizing sensing terminals. Which can spontaneously omitting untrue signal? The rotatable cameras will path the object or people by IPR technology. Simultaneously they triggers alarm to the handheld devices of the central information processing system and security personnel through the sensor network. Interloper's location could be confirmed on the central information processing system electronic alarm and electronic map is trigged. The accident image can get connecting the handheld devices of security personnel and can urgency to the crime scene as initial as possible.

The central information processing system will give lighting facilities and begin to monitoring systems to adhesive tape the entire process in order to confirm the security of the area mainly in the places which is beyond the security personnel sights.

DOI 10.17148/IJARCCE.2016.53169

D. Disaster Alerting and Recovery

In recent times natural disasters like landslide, flood, forest fire etc., and accidental disasters like coal mine accident etc., are taking place more and more regularly. Technologies in internet of things like radio frequency identification and wireless sensor networks could play a crucial role in disaster notifying pervious it happens and disaster recovery after it ends. In command to lessen the belongings of natural disasters such as landslide, flood and forest fire, it is essential to anticipate its occurrence and to alert in time. The timely contact to appropriate data on hazardous environmental conditions gives people in the nearing area timely to apply preparedness procedures, reducing the number of casualties derived from the events and alleviating the damage. Wireless sensor networks enabled the processing, acquisition and transmission of environment data from the location where the disaster create to potentially threatened cities. Then this data could be used for authorities to randomly access critical situation and to establish resources [15]. In accidental disaster recovery, for illustration, after a coal mine accident occurrence, positioning of trapped workers and instant tracing using radio frequency identification technologies could provide economic loss to the largest extent, timely rescue and lessen casualties. Knowing trapped workers relatively accurate position, the reuse action would be more directing thus is time effective. Apart from the above applicants, many others could be labelled as futuristic since they reply on some sensing, communication, industrial processes and materials there are static to come or whose implementation is static too complex [16]. The greatest appealing futuristic includes city information model, robot taxi and improved game room [17].

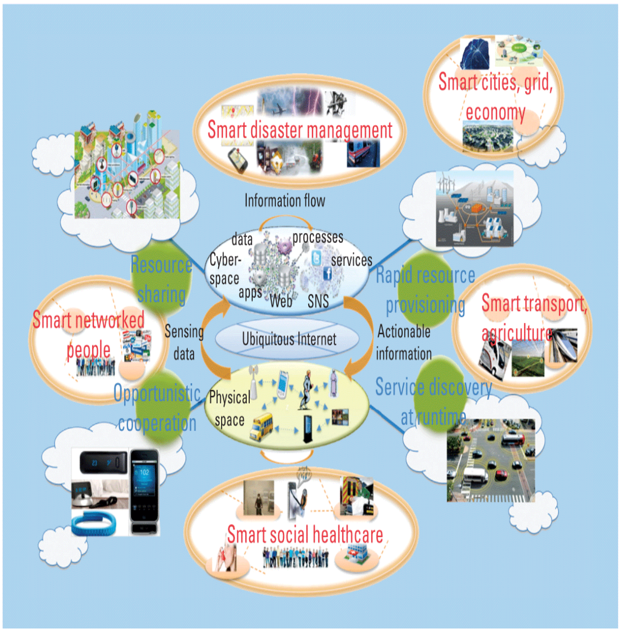


Fig.8 Disaster Alerting and Recovery

VIII. SECURITY CONCERNS IN INTERNET OF THINGS

Internet of things nearly is a network of actual world system with actual time interaction. The development of the original stage of internet of things is machine to machine (M2M) having single characteristics, subscription and deployment contexts. Unattended operation without human intervention is possible from extended periods of time by the WAN (wireless area network) or wireless local area network. Though given that improvements in social effectiveness if makes an array of new problems concerning information security and that breach of privacy [18].

Security concerns in internet of things	
Front end sensors and equipment	1. Unauthorized access to data 2. Threats to the internet 3. Denial of service attack 4. Attack and privacy analysis of M2M or contract information 5. Attacks to availability of M2M or contract information
Network	1. Unauthorized access to data 2. Unauthorized access to service 3. Steal or change to communication information 4. Viruses or malware attacks 5. Network security
Backend of it system	1. Safety management of code resources 2. Replacement of operator

Table.3 Security threads of internet of things

A. Front end sensors and equipment

Front end sensors and equipment collect data through the built in sensors. They then transfer the information using machine to machine or module devices, thus attaining networking services of multiple services sensors.

This method includes the security of machines with node connectivity and business implementation [18]. Perception nodes or machine are mostly dispersed in the nonappearance of monitoring scenario. As invader can easily access these devices which implies damage or illegal actions on these nodes can be done. Potential threats are examined and are categorized to illegal access to information, threats to the denial of service attack and internet.

B. Networks

Networks acting a significant role providing a more comprehensive effect, interconnection capability and thriftiness of connection, as healthy as authentic quality of service in internet of things. Later a maximum number of machines transfer data to large number of nodes, network congestion and group exist in internet of things may be produced in denial of service attacks.

C. Backend of its System

Back end it system form the middleware, gateway, which has gathering and high security requirements, pseudo real time to increase business intelligence or examining sensor data in real time. The security of internet of things system has seven main standard; data integrity, privacy protection, communication layer security, data confidentiality, access control, user authentication and comfort of use at any time.

IX. PRIVACY CONCERNS IN INTERNET OF THINGS

The internet security glossary [19] defines privacy as the right of entity acting in its own to define the degree to which it will interact with its environment, as well as the degree to which the object is willing to share data about itself with others. Typically in internet of things, the environment is detected by connected devices. Then they broadcasts the collected information's and detailed events to the server which carrier out of the applications logic.

This is achieved by fixed communication or mobile which take responsibility. Privacy should be safe in the device, in processing which helps to disclose the sensitive information and at storage during communication [20]. The privacy of data protection and users has been recognized as one of the significant challenges which need to be addressed in the internet of things.

X. CONCLUSION

In this paper, we survey the state of art on the internet of things, including the elements, evolution, applications, challenges, security and privacy. It is held that in the new future the reaching of the vision of anyplace, anytime connectivity for anyone, we will currently have connectivity for anything should determine on cooperative efforts and cross discipline in related field.

REFERENCES

[1] C. Perera., A. Zaslavsky., P. Christen., and D. Georgakopoulos., "Context Aware Computing of the Internet of Things: A Survey," IEEE Communications Survey & Tutorials, 2013, pp.1-41.

[2] L. Atzori., A. Iera., and G.Morabito., " The Internet of Things: Survey," Computer Networks Journal 54(2010), pp.2787-2805.

[3] S. Schneider (2013, October 9) "Understanding the Protocol Behind the Internet of Things [Online]," Available:http://electronicdesign.com/embedded/understanding-protocols-behindinternet-things.

[4] M. Chaqfeh., and N. Mohamed., "Challenges in Middleware Solution for the Internet of Things," IEEE 2012 International Conference on Collaboration Technologies and System (CTS), pp. 21-26.

[5] "IOT/M2M Protocols [online]," Available: http://IOT.eclipse.org/protocols.html.

[6] S. Schneider.,(2013,October 9) "Understanding the Protocol behind the Internet of Things [online],"Available: http://electronicdesign.com/embedded/understanding-protocols-behindinternet-things.

[7] M. Shiuan., and Y.Chee. (no date) "Zigbee Wireless Sensor Networks and Their Applications [online],"Available: http://people.cs.nctu.edu.tw/~yctseng/papers.pub/book-zigbee.pdf.

[8] J. Tan., G. Simon., and M. Koo., "A Survey of Technologies Internet of Things," 2014 IEEE International Conference on Distributed Computing in Sensor Systems, pp. 269 – 274.

[9] Z. Shelby., and C.Bormaan., "6LoWPAN: The Wireless Embedded Internet Companion," Welly Publication 2009.

[10] N. Kushalnagar., G. Montenegro., and C. Schumacher., " IPv6 over Low- Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goal [Online]" Available:http://datatracker.ietf.org/doc/rfc4919/?include_text=1.

[11] Z. Shelby., K. Hartke., and C. Bormann., "The Constrained Application Protocol [Online]," Available: https://tools.ietf.org/html/rfc7252.

[12] A. Vilamovska., E. Hattziandreu., R. Schindler., C. Van Oranje., H. De Vries., and J. Krapelse., "RFID Application in Healthcare-Scoping and Identifying Areas for RFID Deployment in Healthcare Delivery." RAND Europe, February 2009.

[13] L. Ni., C. L.i, L. Qiong., N. Hoilun., and Z. Ze., "Status of the CAS/HKUST Joint Project BLOSSOMS," Proc. Of the 11th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, pp. 469–474, August, Hongkong (China), 2005.

[14] J. Liu., and L. Yang., "Application of Internet of Things in the Community Security Management," Computational Intelligence Communication Systems and Networks, Third International Conference on IEEE, 2011, pp. 314-318.

[15] M. Castillo-Effen., D. Quintela., R.Jordan., W. Weshoff., and W. Moreno., "Wireless sensor networks for flashflood alerting," Proc. Of the 5thIEEE International Caracas Conference on Devices, Circuits and Systems, November, Dominican Republic, 2004.

[16] L. Atzori., A. Iera., and G. Morabito., "The Internet of Things: A survey,"ComputerNetworks,doi:10.1016/j.comnet.2010.05.010,2010.

[17] SENSEI FP7 Project., Scenario Portfolio., User and Context Requirements., Deliverable 1.1, <http://www.senseiproject.eu/>.

[18] D. Jiang., and C. ShiWei.,, "A Study of Information Security for M2M of IoT," 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010, pp. 576-579.

[19] RFC 2828., "Internet Security Glossary," May 2000, [Online]. Available: https://www.ietf.org/rfc/rfc2828.txt.

[20] Y. Cheng., M. Naslund., G. Selander., and E. Fogelström., "Privacy in Machine-to-Machine Communications: A state-of-the-art survey," International Conference onCommunication Systems (ICCS), Proceedings of IEEE, 2012, pp. 75-79.

[21] J. Sathish Kumar., Dhiven R.Patel., " A Survey on Internet of Things: Security and Privacy Issues," International Journal of Computer Application (0975-8887) Volume 90-No 11, March 2014.

[22] Hetal B Pandya., Tushar A Champaneria, "Internet of Things: Survey and Case Studies," IEEE 2015.

[23] Ashvini Balte., Asmita Kashid., Balaji Patil., " Security Issues in Internet of Things (IOT): A Survey," International Journal of Advance Research in Computer Science and Software Engineering, ISSN 2277 128X, vol 5, Issue 4, 2015.

BIOGRAPHIES

M.Suruthi received Bachelor degree B.E computer Science and engineering from Kings college of engineering, Anna University, Chennai. She is now pursing Master's degree M.E computer science and engineering department at SRM Valliammai engineering college, Anna University, Chennai.

D. Nivetha received Bachelor degree B.E computer science and engineering from Jeppiaar SRR engineering college, Anna University, Chennai. She is now pursuing Master's degree M.E computer science and engineering department at SRM Valliammai engineering college, Anna University, Chennai.

DOI 10.17148/IJARCCE.2016.53169