Implementation of RFID with Internet of Things

A.Sivanesh Kumar, S.Brittoraj, M.Rajesh

Abstract*: Internet of Things (IOT) can be defined as a thing or device, physical and virtual, connected and communicating together, and integrated to a network for a specific purpose. The IoT uses technologies and devices such as sensors, RFID (radio frequency identification) and actuators to collect data. IoT is not only about collecting data generated from sensors, but also about analyzing it. IoT applications must, of necessity, keep out all attackers and intruders so as to thwart attacks. IoT must allow for information to be shared, with every assurance of confidentiality, and is about a connected environment, where people and things interact to enhance the quality of life. IoT infrastructure must be open source, without ownership, meaning that anyone can develop, deploy and use it. The objective of this paper is to discuss the various challenges, issues and applications confronting the Internet of Things. The world has shrunk considerably with the dramatic growth in Internet usage. Every computer and mobile phone in the world can be connected together through Internet technology. As a result, intelligent devices are connected and communicate together. The Internet of Things envisions a future where people and intelligent systems cooperate and work together. In the IoT, machine-to-machine communication helps devices exchange data, requiring power, efficiency, security and reliability. This paper advances new ideas for designing a security protocol in the IoT so as to facilitate secure machine-to-machine communication.

***Index Terms*: Internet of Things; Architecture.**

I. INTRODUCTION

Connect and interact together securely. The IoT is born of the recent growth in Radio Frequency Identification (RFID), smart sensors, communication technologies and Internet protocols. The IoT comprises basic building blocks like Wireless Sensor Networks (WSNs), Low-power Wireless Personal Area Networks (LoWPANs), Machine-to-Machine Communication (M2M) and RFID. M2M makes communication between devices with a remote computer. But IoT goes beyond on M2M and makes things connecting with the systems and people. The IoT can be used in a range of applications like supply chains, smart healthcare, smart cities and smart homes. For example, in smart healthcare, patients are continuously monitored by physical objects. Smart homes have doors that open automatically when the inmates arrive, and food prepared and served, as well as assorted smart appliances that make life easy. Radio Frequency Identification (RFID) plays a lead role in the IoT because it identifies any number of objects simultaneously. Since objects in the IoT exchange information together, it is mandatory to keep a record of all the information and track data travel from one object to another. IoT sensors are used for pressure, temperature, humidity and proximity sensing applications. The IoT uses antennas like chip, wire, whip and proprietary.

The IoT integrates new applications from different environments together to support the process of intelligent decision making. The IoT causes physical objects to see, hear, think, interact and talk together to share data. In addition to the above, devices need to be made in line with customers' demands, and so the most compatible heterogeneous applications are created. The IoT delivers quality products to customers, and offers lots of marketing opportunities because IoT-based services show upwardly mobile economic growth. Fig. 1 shows the economic growth of IoT applications in the market. The IoT is looking to earn millions of dollars in business and marketing opportunities, and is a platform that mostly operates on wireless personal area networks. Internet Protocol-based communication is used in the current Internet architecture. However, IoT applications use the ubiquitous connectivity of machines or devices which can sense the surrounding environment. The IoT field continues to look for a standardized protocol and security mechanisms for device-to-device communications.

The IoT is capable of connecting billions or trillions of different devices through the Internet, so long as there is tight synchronization and high-signal communication between IoT devices. Since precious information is shared between devices, it is necessary to incorporate security and privacy in the IoT platform. The IoT supports a wide range of applications like smart homes, smart lighting in streets, smart traffic control, smart traffic congestion detection, and smart cities.

II. LITERATURE REVIEW

Oladayo Bello et. al18 (2016) discussed issues - like sharing, forwarding information, and security - present in device-to-device communication in the Internet of Things. Multifarious challenges present in device-to-device communication were also touched on. Radio frequency identification (RFID) is used to locate real-time objects, and that is precisely its purpose. Daqiang Zhang et al.6 (2016) proposed a new RFID-based method to identify objects.

Zhangbing Zhou et al.26 (2016) proposed a novel method-based Internet of Underwater Things to discover plants and animals present on the ocean floor. Yi Xu et al.23 (2016) introduced cloud-edge-beneath architecture and presented its salient scalability features. Research in wireless

Revised Manuscript Received on December 22, 2018.

A.SivaneshKumar,Assistant Professor, Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamilnadu, India
S.Brittoraj,Assistant Professor, Department of Computer Science and Engineering, Rrasse College of Engineering, Chennai, Tamilnadu, India
M.Rajesh, Professor, Department of Computer Science and Engineering, KRS College of Engineering, India, Raga Academic Solutions, Chennai, India

sensor networks is growing rapidly, and issues such as information-sharing, decision-making, and routing protocols are considered. Keshav Sood et al.13 (2016) advanced significant developments in the Internet of Things in wireless sensor networks.

Huadong Ma et al.10 (2016) analyzed the two biggest challenges in the Internet of Things: interconnecting large-scale heterogeneous network elements, and exchanging data efficiently. The authors presented key aspects like the architecture of the IoT, internetworking models and sensor networking modes. Michele Nitti et al.14 (2016) propositioned a review of virtual objects in the IoT platform, with middleware facilitating and managing the interaction between them. Mohammed Abdur Razzaque et al.15 (2016) projected the challenges of using middleware in the IoT.

Constantinos Kolias et al.3 (2016) posited security issues and the need for security in the Internet of Things. Maria Rita Palattella et al.16 (2016) considered technological and standardization aspects and analyzed the potential of 5G technologies for the Internet of Things. The authors identified synergy and mutual shaping between 5G and the IoT and the role of 5G in IoT infrastructure.

Yunchuan Sun et al.24 (2016) encouraged the concept of SCC (Smart and Connected Communities), which focuses on preservation and revitalization (of the past), the requirements for living in the present, and the need to plan for the future to ensure a sustainable environment. The IoT is able to offer a ubiquitous network of connected devices and smart sensors for SCCs. Dusit Niyato et al.4 (2016) addressed data management in the IoT through a smart data pricing approach. The authors proposed a new pricing scheme for IoT service providers, taking into account purchases of sensing data and service subscription with bundling.

David Park et al.5 (2016) analyzed the role of big data analytics in ensuring the smooth rollout and success of IoT products in multiple business markets. Mohamed Essaid Khanouche et al.17 (2016) analyzed a major issue in the IoT, which is energy and the quality of service in the context of IoT service composition. Further, the authors proposed a new algorithm called the EQSA (energy-centered and QoS aware) which preselects services and reduces the energy consumption of a composite service.

Philip Laplante et al.19 (2016) presented challenges and issues in healthcare monitoring in hospitals. Pawani Porambage et al.20 (2016) propounded security and privacy issues in the Internet of Things at the design level in various applications. Glenn Parsons8 (2016) propositioned the application and standardization of machine-to-machine communication in industries. Aref Meddeb2 (2016) proffered a survey of IoT service definition, standardization and regulation activities. Also, the author underscored the need to unify protocols, services and standards for the IoT, as well as the efforts taken by diverse organizations. Guiou Kobayashi et al.9 (2016) posited the ethical prospects of the IoT and suggested that technological evaluations and social relationships would become cheaper with advancements in IoT technologies. Amir Vahid Dastjerdi et al.1 (2016)recommended the application of the IoT in multifarious fields, and dwelt on issues in the current storage system, and handling huge volumes of data, from the perspectives of fog and cloud computing.

Sara Amendola22 (2014)discussed the support of fog computing in the IoT environment. Jonathan Margulies12(2015)raised various research issues in the field of the IoT and advanced the importance of security and privacy of information in the IoT. Huadong Ma11 (2016)projected the architecture of the IoT and discussed integration between devices. Yuvraj Agarwal25(2016)touched upon the importance of encrypting information shared in the IoT. Phillip A. Laplante21(2016)presented a case study for disaster response using the IoT. David Metcalf7 (2016)propositioned the importance of the IoT to set up smart healthcare hospitals.

III. CHALLENGES IN IOT

Going forward, advancements and developments in the IoT will culminate in smart homes, cities, and cars. The use of the word smart presupposes that a lot of issues will have to be considered, such as the use of sensor devices, storage data, service costs, programming smart appliances, running applications, and the like. We analyze these to devise cloud sensor systems, with massive numbers of sensors and devices to be integrated into cloud-based sensor systems. The first challenge in creating a smart environment is to integrate devices and establish communication among them. Building real-time IoT-based smart devices will require the integration of countless mechanisms, sensors and supplementary technologies. Another challenge in the smart environment is to integrate and transform data among devices. Consequently, the need for cloud sensor storage architecture is raised when smart environments are designed. When designing these, incoming and outgoing traffic is to be reckoned with, because hundreds of sensors and devices are connected together. Every second, those devices and sensors communicate and interact together, based on the events in question. A lot of devices work, depending on the life of the battery. It is necessary, therefore, to make smart environments in the IoT reliable. Fig. 1 shows a smart healthcare application in the IoT. IoT device is able to sense the heart rate and respiratory rate. When there is abnormalities arise, immediately it alerts the doctor and other responsible persons.

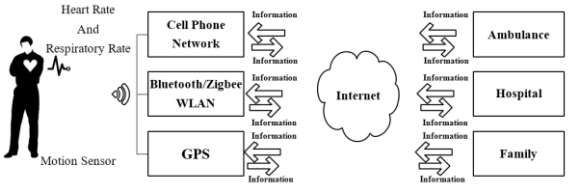

Fig. 1. A Smart Healthcare Application

3.1 Security and Privacy in the IoT

Owing to the large numbers of different devices in use, security must provide an access control mechanism and policy. The behavior of devices in the IoT is dictated by safety concerns, and calls for a special model to track their behavior. This challenge has come about as a result of heterogeneity. Security and privacy challenges in the IoT are a more prominent concern, compared with traditional networks. With almost everything connected to the internet, much of the information sought is intrusive and invades the privacy of users, so protection of privacy becomes a key security issue in the IoT. Given that the IoT is a combination of things,

services, and networks, its security needs to cover more management objects and levels than traditional network security. Current security architecture is designed from the perspective of human communication, which may not be suitable and directly applicable to the IoT system. Using the currently-existing security mechanisms will likely block the logical relationships between things in the IoT, which needs low-cost, M2M-oriented technical solutions.

A natural characteristic of an IoT environment is the prevalence of devices, sensors, readers, and applications with the potential to collect a multiplicity of data types of individuals as they move through such an environment. The possibility of automatically identifying objects may lead to an automatic identification of persons related to these objects. The information collected - based on object identifiers, sensor data and the connection capabilities of IoT systems - might therefore reveal information on individuals, their habits, location, interests and other personal information and preferences stored for the ease of use in systems.

There are certain security threats in the IoT like the leakage of personally-identifiable information and sensitive user information, in addition to unauthorized execution of tasks. One of the desirable features of the IoT is user and location awareness in large environments. Today, technologies like the bluetooth and Wi-Fi have advanced the capture of location awareness. Information about patients in hospital, for instance, is valuable and very sensitive user data. In the IoT, it is necessary to prevent the leakage of this kind of sensitive user information. IoT data application data may be transmitted as plaintext. If user information is not encrypted by means of effective cryptographic algorithms, there is every likelihood that it may be captured by hackers. Many IoT products are unable to support cryptographic functions because they are inexpensive and have few computational. The threat to the IoT environment is doubly high, because it is connected in the real world and countless plug-and-play devices can be used. Therefore, to prevent data breaches in an IoT environment, it is advisable to set up foolproof security protocols.

3.2. Middleware in IoT

The primary characteristic of the IoT is that it comprises a large-scale network of things and devices from various environments that can be connected and capable of communicating together through events. From this viewpoint, the support of middleware is fundamental to integrate devices from heterogeneous platforms. The IoT offers its services in domains like transportation, healthcare, smart environments, industrial and social services. The IoT is connected with internet technology and each device operates within a particular environment through mutual understanding. Middleware is a software application layer that facilitates and manages interaction between applications from heterogeneous environments. Middleware in the IoT supports functions like resource management, reliability and security. Every device in the IoT will be required to advertise itself as well as the services it offers. Further, the use of the available resources in the IoT must be monitored periodically. IoT middleware supports data management services like data acquisition, storage and compression. Any number of events can take place in an IoT environment, and code deployment in an IoT platform is a challenge. IoT middleware supports event management and code migration services.

IoT middleware needs to be scalable and provide real-time services. Information is to be delivered reliably and swiftly. If there is a failure in the IoT network, it is to be corrected immediately or alternate available resources used. Middleware must work with heterogeneous devices, without additional effort from the application, and facilitate the exchange of information across the network. Built on a dynamic and changing environment, middleware should offer new services with advanced functions based on the changing environment, be adaptive to change and entirely self-functioning.

3.3. Fog Computing in IoT

The IoT generates huge quanta of data that call for special requirements and resources to manage it. Data generated by the IoT can be helpful when analyzed. Cloud computing could help, in many cases, by offering large storage and processing infrastructure, but for special cases like healthcare, emergencies, and miscellaneous time-sensitive applications, delays that occur at the time of data transfer to the cloud and back to the application play a critical role.

The IoT allows devices, sensors, and people to be part of the internet, leading to new forms of communication between humans and things, as well as machine-to-machine (M2M). Even the cloud, as a solution, is insufficient to meet the needs of the data generated. Fog computing is designed to handle precisely such an issue. Basically, it provides the cloud as a service to the network edge, and elevates cloud and edge resources along with its own infrastructure.

It facilitates the management of networking and storage services. Furthermore, it supports user mobility, resources from different platforms, and data analysis. The applications of fog computing in the IoT help provide smart utility services and healthcare monitoring.

IV. ISSUES IN THE IOT

4.1. Data Storage in the IoT

Obviously, the IoT generates large quantities of data every day, and sends them to the provider for the purpose of analyses. But where exactly do enterprises plan to store massive amounts of retrieved data? According to researches, there will be an estimated 26 billion units installed globally by 2020, with many more on the way in succeeding years, as the price of processors drops. In the near future, it will be feasible to install a processor into just about everything.

Where is all the data provided by all of those processors going to be stored, and what problems are likely to crop up around them? This is not just a brainteaser, but a very practical and real problem. After all, if enterprises are to get the bountiful insights into customer activity that the IoT promises, they are also going to have to keep all that information somewhere while it is being analyzed.

Successful implementation and deployment of the IoT will generate large quantities of data that need to be processed and analyzed in real time, increasing time complexity and maximizing workloads at data centers, putting providers in jeopardy in terms of security issues and capacity, as well as confronting challenges to analytics.

V. IOT ARCHITECTURE

A typical IoT architecture (Khan et al. 2012, Yang et al. 2011, Wu et al. 2010) has five layers. They are: an objects layer, an object abstraction layer, a service management layer, an application layer, and a business layer.

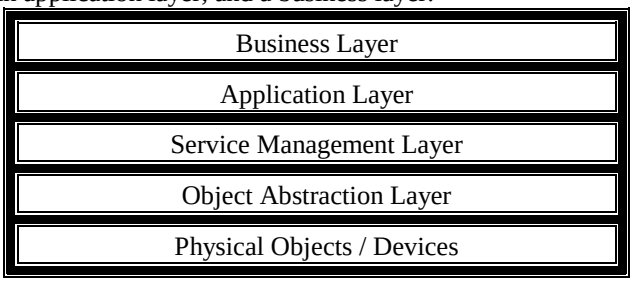

Fig. 2. IoT Architecture

As shown in Fig. 2, the key layer in an IoT architecture is the Object Abstraction Layer, with lots of devices connected together. These devices communicate with each other and share information. This layer comprises different sensors and actuators that perform functions like finding locations and ascertaining temperature, heat, motion, vibrations, and the like. Further, this layer offers plug-and-play devices.

The purpose of the object abstraction layer is to transfer information collected by assorted devices securely, and uses technologies like the RFID, Bluetooth, and WiFi. The Service Management Layer is responsible for pairing services based on the requestor's address and name. The Application Layer offers IoT services based on requests from customers that involve smart homes, smart hospitals, smart cities, and so on. Finally, the Business Layer controls and manages the overall IoT system's activities and services. The function of this layer is to devise business models, graphs, and flowcharts. It also monitors information shared between devices.

VI. IOT ELEMENTS

There are six main elements (Pilkington 2014, Rushden 2012) needed for IoT functionality, as shown in Fig. 3. Identification is mandatory to discover objects in the IoT environment. Identification is carried out using the unique address of a particular object, or to locate a particular service, based on customer requirements. To collect data, an IoT sensing mechanism is used. It gathers information from authorized objects and sends it back to the data warehouse or database.

Communication technologies connect devices from different environments, using communication protocols like WiFi, Bluetooth, and the IEEE 802.15.4, as well as communication technologies like the RFID and NFC. The RFID reader sends a query signal to the tag, receives a reflected signal from the tag, and passes it on to the database. The database approaches a processing center to find objects based on the reflected signals within a certain range. WiFi technology is also used to exchange information between objects.

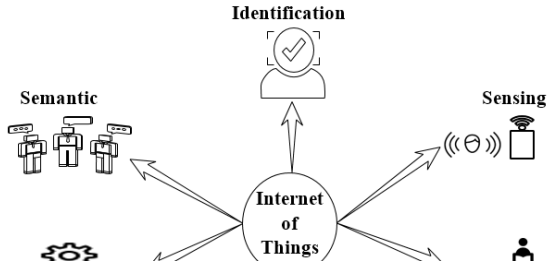

Fig. 3.IoT Elements

Organizations and companies use smart hubs and mobile applications that help people monitor the IoT platform. IoT

Processing units and software applications are the brain of the IoT. Processing units include microprocessors and microcontrollers. Additionally, real-time operating systems are used to run the objects in question. IoT services (Xiaojiang et al. 2010, Gigli et al. 2011) are divided into identity-related services, information aggregation services, ubiquitous services and collaborative-aware services. Identity-related services bring real-world objects into the virtual world to have the objects identified. Information aggregation services collect the information sensed from objects. Collaborative-aware services make intelligent decisions based on the sensing information gathered. For example, smart home services reduce the workload of the average resident by automatically opening doors, shutting windows, and switching off lights and fans. Smart healthcare services monitor the status of patients' health. Semantic services, referred to as knowledge extraction, include identifying and analyzing data to take appropiate decisions to provide the precise services called for.

VII. MAJOR APPLICATIONS OF THE IOT

The smart home is a leading IoT application. Plenty of users have opted for smart homes and companies are coming up with an array of Internet of Things-based smart home applications. To measure air quality inside and outside the home, a sensor is used to obtain NO2 and CO levels outside. Given this data, the quantum of air pollution can be calculated. The data captured using this sensor is sent through WiFi technology, and the graphs drawn show the level of air pollution. Wearables are hot on the Internet of Things. A sensor band that tracks location data and food logging, for instance, can be worn on the hand. A similar wearable device analyzes users' heart rate to determine abnormal heart conditions. Fig. 4 shows a list of applications supported by the Internet of Things.

Smart Cities aim to make cities safer and cleaner. The purpose of a smart city in the IoT is to analyze traffic and monitor pollution of all sorts - noise, air, land and water - as well as track waste management. Smart cities also monitor the length and breadth of the city to reduce crime. The IoT is also effectively used in Smart Retail. Smart retail functions include the point of sale; mobility; inventory transfers; pricing; analyzing goods, as well as monitoring staff activity, purchasing, and sales history. Smart Health monitors the status of patients continuously. Patients with heart disease, cancer and diabetes are periodically monitored by smart health IoT devices and reports sent to doctors.

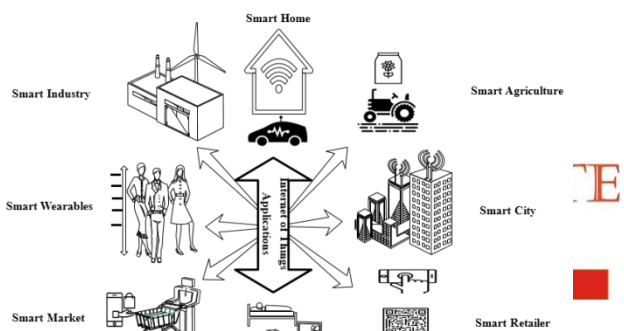

Fig. 4. IoT: Applications

VIII. CONCLUSION

In this paper, the challenges, issues and applications to do with the IoT are presented. Device-to-device communication is at the centre of an IoT environment in designing and sharing information in an IoT ecosystem, with the latter stored in the cloud. The information retrieved from the IoT ecosystem is to be shared in a secured and a reliable framework. Efficient cryptographic algorithms can be used to encrypt information. The purpose of middleware in the IoT is to connect applications from different environments. This paper concludes that the IoT will, going forward, provide a first-rate living environment for people everywhere.

REFERENCES

1. Amir Vahid Dastjerdi and Rajkumar Buyya, "Fog Computing: Helping the Internet of Things Realize Its Potential", IEEE Communications Society, August 2016.
2. Aref Meddeb, "Internet of Things Standards: Who Stands Out from the Crowd?", IEEE Communications Magazine - Communications Standards Supplement, July 2016.
3. Constantinos Kolias and Angelos Stavrou, Irena Bojanova, and Richard Kuhn, "Learning Internet of Things Security Hands-on", Copublished by the IEEE Computer and Reliability Societies, January/February 2016.
4. Dusit Niyato, Dinh Thai Hoang, Nguyen Cong Luong, Ping Wang, Dong In Kim, and Zhu Han, "Smart Data Pricing Models for the Internet of Things: A Bundling Strategy Approach", IEEE Network, March/April 2016.
5. David Park, "The Quest for the Quality of Things: Can the Internet of Things deliver a promise of the quality of things?", IEEE Consumer Electronics Magazine, April 2016.
6. Daqiang Zhang, Laurence Tianruo Yang, Min Chen, Shengjie Zhao, Minyi Guo, and Yin Zhang, "Real-Time Locating Systems Using the Active RFID for the Internet of Things", IEEE Systems Journal, Vol. 10, No. 3, September 2016.
7. David Metcalf, Sharlin T. J. Milliard, Melinda Gomez, and Michael Schwartz, "Wearables and the Internet of Things for Health", IEEE Pulse, September / October 2016.
8. Glenn Parsons, "The Internet of Things", IEEE Communications Magazine, July 2016.
9. Guiou Kobayashi, Maria Eunice Quilici-Gonzalez, Mariana Claudia Broens, and José Artur Quilici-Gonzalez, "The Ethical Impact of the Internet of Things in Social Relationships", IEEE Consumer Electronics Magazine, July 2016.
10. Huadong Ma, Liang Liu, Anfu Zhou, and Dong Zhao, "On the Networking of Internet of Things: Explorations and Challenges", IEEE Internet of Things Journal, Vol. 3, No. 4, August 2016.
11. Huadong Ma, Liang Liu, Anfu Zhou, and Dong Zhao, "On the Networking of Internet of Things: Explorations and Challenges", IEEE Internet of Things Journal, Vol. 3, No. 4, August 2016.
12. Jonathan Margulies, "Garage Door Openers: An Internet of Things Case Study", IEEE Computer and Reliability Societies, July/August 2015.
13. Keshav Sood, Shui Yu, and Yong Xiang, "Software-Defined Wireless Networking Opportunities and Challenges for Internet-of-Things: A Review", IEEE Internet of Things Journal, Vol. 3, No. 4, August 2016.
14. Michele Nitti, Virginia Pilloni, Giuseppe Colistra, and Luigi Atzori, "The Virtual Object as a Major Element of the Internet of Things," IEEE Communications Surveys & Tutorials, Vol. 18, No. 2, Second Quarter 2016.
15. Mohammad Abdur Razzaque, Marija Milojevic-Jevric, Andrei Palade, and Siobhán Clarke, "Middleware for Internet of Things: A Survey", IEEE Internet of Things Journal, Vol. 3, No. 1, February 2016.
16. Maria Rita Palattella, Mischa Dohler, and Alfredo Grieco, "Internet of Things in the 5G Era: Enablers, Architecture, and Business Models", IEEE Journal of Selected Areas in Communications, Vol. 34, No. 3, March 2016.
17. Mohamed Essaid Khanouche, Yacine Amirat, Abdelghani Chibani, Moussa Kerkar, and Ali Yachir, "Energy-Centered and QoS-Aware Services Selection for Internet of Things", IEEE Transactions on Automation Science and Engineering, Vol. 13, No. 3, July 2016.
18. Oladayo Bello and Sherali Zeadally, "Intelligent Device-to-Device Communication in the Internet of Things", IEEE Systems Journal, Vol. 10, No. 3, September 2016.
19. Phillip A. Laplante and Nancy Laplante, "The Internet of Things in Healthcare: Potential Applications and Challenges", IT Pro, IEEE Computer Society, May/June 2016.
20. Pawani Porambage, Mika Ylianttila, Corinna Schmitt, Pardeep Kumar, Andrei Gurtov, and Athanasios V. Vasilakos, "The Quest for Privacy in the Internet of Things", IEEE Cloud Computing, March/April 2016.
21. Phillip A. Laplante, Jefrey Voas, and Nancy Laplante, "Standards for the Internet of Things: A Case Study in Disaster Response", IEEE Computer Society, May 2016.
22. Sara Amendola, Rossella Lodato, Sabina Manzari, Cecilia Occhiuzzi, and Gaetano Marrocco, "RFID Technology for IoT-Based Personal Healthcare in Smart Spaces", IEEE Internet of Things Journal, Vol. 1, No. 2, April 2014.
23. Yi Xu and Abdelsalam Helal, "Scalable Cloud–Sensor Architecture for the Internet of Things", IEEE Internet of Things Journal, Vol. 3, No. 3, June 2016.
24. Yunchuan Sun, Houbing Song, Antonio J. Jara, and Rongfang Bie, "Internet of Things and Big Data Analytics for Smart and Connected Communities", Digital Object Identifier 10.1109/Access, March 2016.
25. Yuvraj Agarwal and Anind K. Dey, "Toward Building a Safe, Secure, and Easy-to-Use Internet of Things Infrastructure", IEEE Computer Society, April 2016.
26. Zhangbing Zhou, Beibei Yao, Riliang Xing, Lei Shu, and Shengrong Bu, "E-CARP: An Energy-Efficient Routing Protocol for UWSNs in the Internet of Underwater Things", IEEE Sensors Journal, Vol. 16, No. 11, June 2016.
27. S.P. Raja, T. Dhiliphan Rajkumar and Vivek Pandiya Raj, Internet of Things: Challenges, Issues and Applications, Journal of Circuits, Systems and Computers, Vol. 27, No. 12, 2018.
28. S.P. Raja, T. Sampradeepraj, Internet of Things: a Research oriented Introductory, International Journal of Ad Hoc and Ubiquitous Computing, Vol. 29, No. 1/2, 2018.
29. Rajesh, M., and J. M. Gnanasekar. "Path Observation Based Physical Routing Protocol for Wireless Ad Hoc Networks." Wireless Personal Communications 97.1 (2017): 1267-1289.
30. Rajesh, M., and J. M. Gnanasekar. "Sector Routing Protocol (SRP) in Ad-hoc Networks." Control Network and Complex Systems 5.7 (2015): 1-4.
31. Rajesh, M. "A Review on Excellence Analysis of Relationship Spur Advance in Wireless Ad Hoc Networks." International Journal of Pure and Applied Mathematics 118.9 (2018): 407-412.
32. Rajesh, M., et al. "SENSITIVE DATA SECURITY IN CLOUD COMPUTING AID OF DIFFERENT ENCRYPTION TECHNIQUES." Journal of Advanced Research in Dynamical and Control Systems 18.
33. Rajesh, M. "A signature based information security system for vitality proficient information accumulation in wireless sensor systems." International Journal of Pure and Applied Mathematics 118.9 (2018): 367-387.
34. Rajesh, M., K. Balasubramaniaswamy, and S. Aravindh. "MEBCK from Web using NLP Techniques." Computer Engineering and Intelligent Systems 6.8: 24-26.