Survey on Challenges and Applications of Internet-of-Things

S. Prince Sahaya Brighty[#], P. Selvanayaki[#], M. Kiruthika[#]

[#]*Assistant Professor,*
Department of Computer Science and Engineering,
Sri Ramakrishna Engineering College, Coimbatore-22, Tamil Nadu, India
[1]brighty.s@srec.ac.in

[#]*Assistant Professor,*
Department of Computer Science and Engineering,
Sri Ramakrishna Engineering College, Coimbatore-22, Tamil Nadu, India
[2] selvanayaki.p@srec.ac.in

[#]*Assistant Professor,*
Department of Computer Science and Engineering,
Sri Ramakrishna Engineering College, Coimbatore-22, Tamil Nadu, India
[3] kiruthika.m@srec.ac.in

***Abstract*—** The Internet of Things (IoT) is the next trend of innovation that potentials to improve and enhance our daily life based on smart sensors and smart objects working together. The primary vision of the IoT was to fundamentally change the way of doing business, developing greater competences, motivating deeper customer networks and presenting new business models. IoT includes devices such as radio frequency identifications (RFID), sensors, and actuators, as well as other instruments and smart appliances that are becoming an essential part of the Internet. It is important to gather accurate raw data in a competent way; but more significant is to inspect and mine the raw data to abstract more valuable information such as relationships among things and services to provide web of things or Internet of services.Devices can be connected to the Internet using unique IP addresses in Internet Protocol (IP) connectivity, hence agreeing them to be read, controlled, and managed at everywhere and every time. Security is a vital aspect for IoT deployments. Due to the robust attacking ability, speed, simple implementation and additional features, differential fault analysis has turn out to be an important method to weigh the security in the Internet of Things. This paper elaborately affords the knowledge on architecture, challenges, security and applications of IoT in various fields.

***Keywords*—** Internet of Things, Smart Sensors, Smart Objects, Internet Protocol, Differential Fault Analysis

I. INTRODUCTION

Internet of Things is a multidisciplinary field and vibrant universal network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'Things' have unique characteristics, physical features, and implicit personalities and practice intelligent interfaces, and are effortlessly included into the information network[1]. The quantities of Internet linked devices are growing at the fast rate. These devices comprises of personal computers, laptops, tablets, smart phones, PDAs and other hand-held embedded devices. Most of the mobile devices embed different sensors and actuators that can sense, carry out computation, make intellectual decisions and communicate valuable gathered information through the Internet.

IoT permits `people and things to be connected Any-time, Any place, with Anything and Anyone, preferably using Any path/network and Any service'[2]. In the direction of designing the robust applications, developers need suitable tools and methods for analysing and handling their applications on existent hardware in large-scale deployments. In the initial days of IoT research, the accessibility of smart devices was inadequate, and only current progresses in technology have improved their accessibility at lower costs. While experimentations were mainly small-scale and done in research laboratories, they permitted for an enhancement in understanding the effect and restrictions of existent hardware on performance of protocols and design ranges.

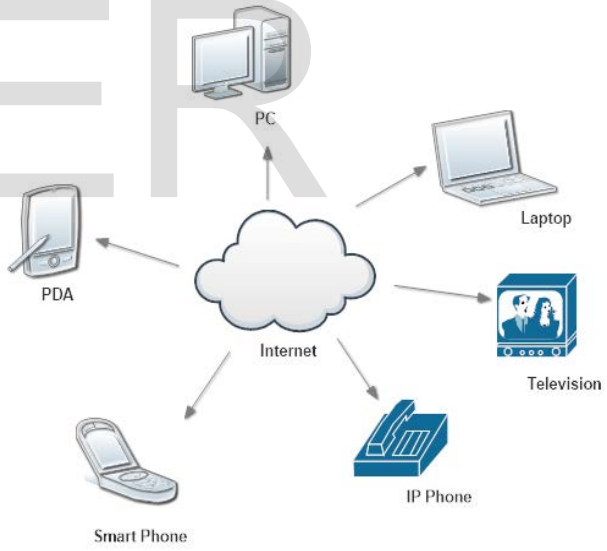

Fig. 1 Internet of Things

Major applications of IoT in diverse areas, such as home automation, industrial automation, medical aids, mobile healthcare, elderly assistance, intelligent energy management and smart grids, automotive, traffic management, and many other service sectors like Smart Governance, Smart Mobility, Smart Utilities, Smart Buildings, and Smart Environment [9].

Nowadays the information security engineers are tackled with the problem of constructing a trustworthy system from

untrustworthy components, particularly in the Internet of Things (IOT). The pervasive device connectivity to the Internet also poses hidden security risks, namely, snooping on the wireless communication channel, unauthorized access to devices, tampering with devices, and privacy risks. Security of the whole system in the IOT is usually provided at the level of software (cryptographic algorithms) [4] and protocols are not easy to install on such devices and still more hard to keep the software up-to-date. The capability to connect, manage, and control a device from anywhere and at any time needs suitable authentication and authorization methods. Security professionals have emphasized the significance of security in IoT deployments and have advised about the insecurity of current deployments [8].

II. IoT ARCHITECTURE

Generally, the structure of IoT is divided into five layers as shown in Fig. These layers are briefly described below:

1) Perception Layer:

The Perception layer is also termed as 'Device Layer'. This layer includes technologies that intellect physical objects and translate them into cyber entities. Major sensing technologies comprise of radio-frequency identification (RFID), radar, infrared induction, the Global Positioning System (GPS), and Wi-Fi, Bluetooth, and ZigBee WSN. In addition to this, it includes mechanical and electronic actuators—valves and switches—that connect to the sensors and execute their instructions. This layer fundamentally deals with the identification and collection of objects specific information by the sensor devices[37]. Depending on the type of sensors, the information can be about position, temperature, direction, motion, pulsation, acceleration, moisture, chemical changes in the air etc. The gathered information is then passed to Network layer for its safe transmission to the information processing system.

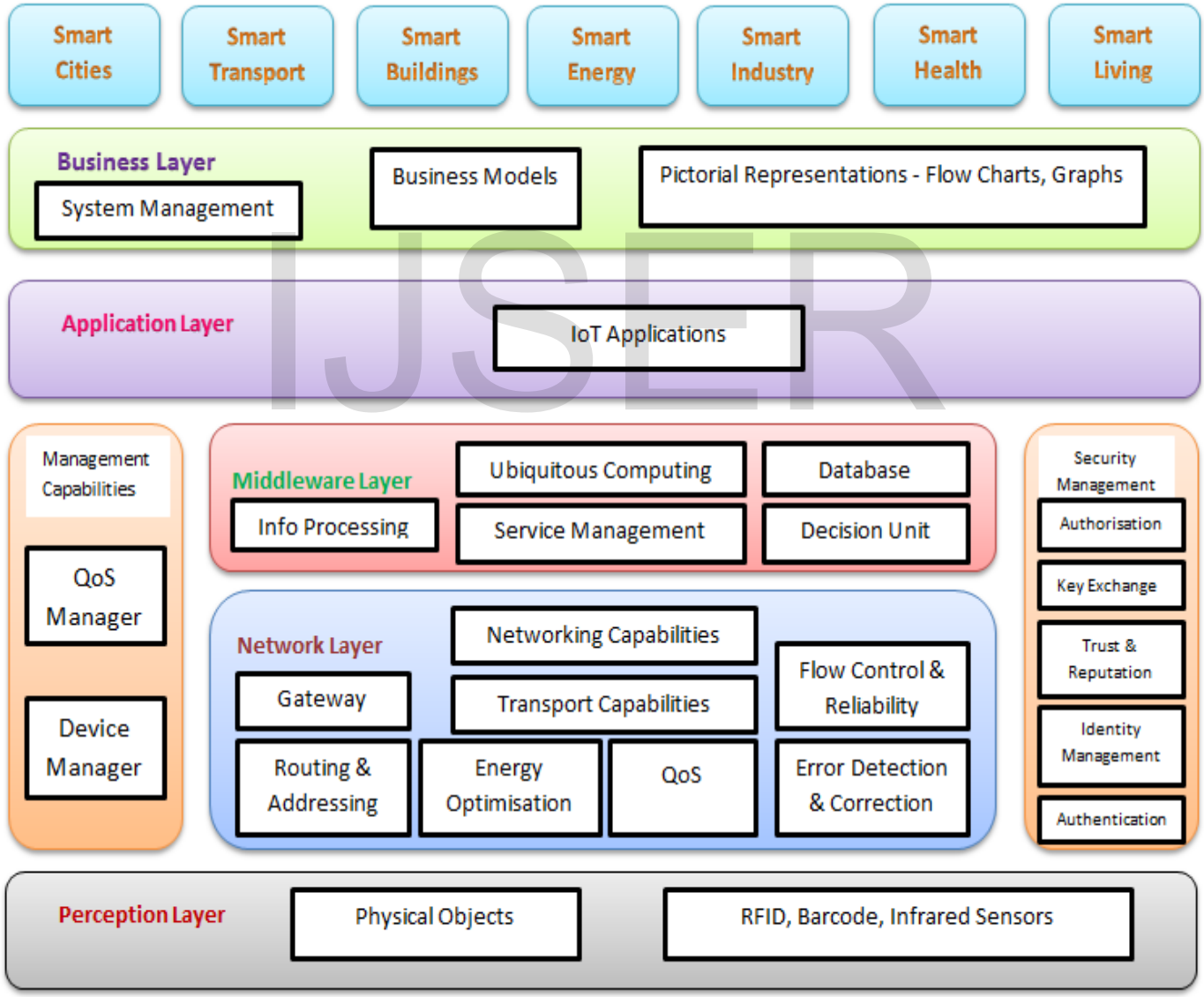

Fig. 2 Architecture of IoT

2) Network Layer:

The Network layer can also be termed as 'Transmission Layer'. The network layer contains all network components like interfaces, routers, and gateways and communication channels. *Management and data centers* operate as nodes in the network, unit M&DCs are under the straight or circuitous manage of local (lM&DC), industrial (iM&DC), and public (nM&DC) entities. Heterogeneous network configurations consist of the Internet, wireless sensor networks and mobile and telecommunications networks. This layer securely transmits the information from sensor devices to the information processing unit. The transmission medium can be wired or wireless and technology can be 3G, UMTS, Wi-Fi, Bluetooth, infrared, ZigBee, etc. depending upon the sensor devices. This layer guarantees trustworthy data transmission in addition to connectivity by applying safe data coding, fusion, mining, and aggregation algorithms. Thus, the Network layer transfers the information from Perception layer to Middleware layer.

3) Middleware Layer:

The device over the IoT executes different type of services. Every device connects and communicates with only those other devices which execute the same service type. This layer is responsible for the service management and has connection to the database. It accepts the information from Network layer and stores in the database. It performs information processing and ubiquitous computation and takes automatic decision depends on the results.

4) Application Layer:

The application layer offers global management of the application depends on the objects information processed in the Middleware layer. This layer supports applications in local, industrial, and national IoTs controlled correspondingly by lM&DCs, iM&DCs, and nM&DCs. A local IoT connects unit IoTs in a geographical region; an industrial IoT manages unit IoTs in an industry such as transportation or telecommunications; and a national IoT integrates a country's local and business IoTs. It also contains service integration, transnational supervision, and global coordination. The applications implemented by IoT can be smart health, smart farming, smart home, smart city, intelligent transportation, etc.

5) Business Layer:

This layer is responsible for the management of whole IoT system including the applications and services. It constructs business models, graphs, flowcharts etc. based on the data received from Application layer. The actual achievement of the IoT technology also depends on the good business models. Based on the analysis of results, this layer will help to find out the future events and business strategies.

A. Different Protocols in IoT:

TABLE I

Protocols	Description
Constrained Application Protocol(CoAP)	A software protocol planned to be used in very simple electronics devices that allow them to commune interactively over the Internet. It is predominantly targeted for small low power sensors, switches, valves and related components that must be controlled or managed remotely, through typical Internet networks. CoAP is an application layer protocol that is proposed to make use of resource-constrained internet devices, such as WSN nodes. CoAP is designed to simply transform to HTTP for simplified integration with the web, however to meet the specific necessities such as multicast support, especially low overhead, and simplicity.
Representational State Transfer (REST)	A way of software architecture for distributed systems such as World Wide Web. REST has come out as a leading web API design model.
Message Queue Telemetry Transport(MQTT)	An open message protocol for M2M communications that allows conveying the telemetry-style data from pervasive devices, beside high latency or constrained networks, to a server or small message agent.
The Extensible Messaging and Presence Protocol (XMPP)	An open technology for real-time communication, which influences a broad range of applications including instant messaging, presence, multi-party chat, voice and video calls, collaboration, lightweight middleware, content syndication, and universal routing of XML data.

B. COMPONENTS:

TABLE III

Components	Description
IPv4 and **IPv6**	Internet Protocol version 6 (IPv6) is the latest revision of the Internet Protocol (IP), the communications protocol that gives an identification and location system for computers on networks and routes traffic across the Internet.

	Each device on the Internet must be allocated an IP address to communicate with other devices. With the rising number of novel devices being connected to the Internet, the need arose for more addresses than IPv4 is able to accommodate. IPv6 utilizes a 128-bit address, permitting 2128, or roughly 3.4×1038 addresses, or more than 7.9×1028 times as many as IPv4, which makes use of 32-bit addresses.
UDP	The User Datagram Protocol (UDP) is one of the core members of the IP suite. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network lacking prior communications to set up special transmission
TCP	The Transmission Control Protocol (TCP) is intended to make use as a greatly reliable host-to-host protocol between hosts in packet-switched computer communication networks, and interconnected systems of such networks
6LoWPAN	6LoWPAN is an acronym of IPv6 over Low power Wireless Personal Area Networks. The 6LoWPAN group has described encapsulation and header compression mechanisms that allow IPv6 packets to be sent and received from over IEEE 802.15.4 based networks.

III. CHALLENGES IN IOT

A. *CHALLENGES in IoT- EXPERIMENTATION*

The main objective of IoT research is to put together the island of WSN technologies into a worldwide interconnected infrastructure, moving from the presently existing *Intra*-net to a real *Inter*-net of Things. The resultant challenges are (i) Increase in *scale* (ii) Increase in heterogeneity of devices and device technologies. (iii) Increased in *concurrency* of access to the infrastructure. (iv) Propose a mechanism to hold adequate *user involvement.*

These challenges need novel approach to support interoperability at different layers of the communication heap for resource-constrained devices, which have to be sufficiently reflected in IoT experimentation environments.

B. *TECHNICAL CHALLENGES OF IOT:*

Although there is a difference in dealing of mining issues for the IoT from the traditional mining problems, they still take over many of the open issues in the development of the mining algorithms for IoT, such as scalability for large-scale data set.

1) Infrastructure Perspective:

Decentralization and *heterogeneity*, of IoT have strong impact *in* the development of data mining algorithms. We need to rethink how to decentralize mining technologies for the IoT. A classic instance of clustering for WSN is most of the traditional clustering algorithms are intended to execute on a single system (centralized) with all the available data, they actually are inappropriate for saving the power of sensors of a WSN. Another instance is the classification algorithm for IoT which also endures from the issue of decentralized computing. There is no need to distribute all the computations to several things (i.e., sensors or devices), it will not carry all the benefits of using the decentralized strategy. Hence, whether to decentralize or not depends on the application, the system, or the application domain. It shows that the centralized computing on a local site (i.e., a group of devices) and the distributed computing on the global site (i.e., the application or system) may ease the change of traditional mining technologies to the IoT environment with a minimum number of changes.

2) Data Perspective:

To process the *large-scale* data entering the system from *different data resources quickly* and *dynamically*, several relevant technologies, such as data preprocessing, information extraction, and information retrieval are generally employed. The major issues are

(i) limited memory size

(ii) interoperability and interactivity between things

The solutions for these issues are needed to filter out unnecessary data using dimension reduction, data compression, and data sampling to avoid their influence on the performance of the system. Data obtained from many resources do not utilize the similar interpretation process, which might be origined by different level of representation or different relational data. Ontology, semantic web, extensible markup language (XML), and additional associated technologies appear to be able to give a clarification to increase the interoperability and interactivity between things. Besides ontology, semantic web, XML, ADL, IADL, and additional associated technologies, the collective intelligence (CI) for the internet can improve the ontology and semantic web technologies to automatically or semi automatically make the knowledge base to depict and identify the particular patterns (i.e., association rules) since a few of the human knowledge and wisdom can be found on the internet.

3) Algorithm Perspective:

Since sensors or devices may connect or leave the system at any time or the network topology may be changed, the characteristics of data that need to be analyzed are not always the same or static. In some cases, the stream data will enter the system not at the same time. Dynamically adjusting the mining results and rerunning the mining algorithm are two perceptive ways to solve the problem faced in a dynamic environment, but both approaches increase the computation time. A static system may have a lower accuracy rate because it cannot handle the events which are not predefined for the system, such as the invasion of strangers. A dynamic mining algorithm may be used except that the thresholds or conditions for adding classifiers or for adjusting the classifiers of such a system can be made more restrictive to retain the accuracy rate while providing the flexibility. The open problems on the combination of diverse mining technologies are: how the data from a mining algorithm (or module) are transferred to another and how the computation load and services are balanced.

Another critical issue is over fitting, it is not caused by the mining problems but by the mining algorithms. For example, although the labeled patterns act like the knowledge base (experience or knowledge from experts) of the system that can be used to construct the classifier (model) to classify the unlabeled patterns, the answer to how many patterns are needed to train the classifier is not unique. The more the training patterns, the higher the accuracy rate. This can be easily guaranteed by examining that a larger number of training patterns involves a more precise training. Labeling patterns is very costly in terms of the computation time or cost. Thus, the number of training patterns used depends to a large extent on the desire to achieve a balance between cost and accuracy. This is due to the reason that some mining algorithms employ iterative process to find the solutions, after too many iterations of training, the candidate solutions created by the mining algorithms may fit too well to the training patterns. This type of situation takes place not only on the traditional mining algorithms but also on the metaheuristic based mining algorithms. For this reason, to avoid falling into local optimum at the early iterations, the timings to restart the mining algorithms, to alter (i.e., to delete, add, or modify) the candidate solutions, and to choose the features are the main issues on more training, which may have a good impact on the mining technologies of IoT.

4) Trust and Privacy:

Although some of the camera-based detection and recognition technologies are mature enough, the privacy of users will create the majority of people uncomfortable. Similar concerns when using data mining technologies to evaluate the data from IoT appear in recent years. For example, companies today can easily assemble various kinds of data of consumers from different sources or devices and then use data mining technologies to discover the information that can be used to formulate marketing tactics to enhance the volume and revenue of sales, but the truth is that not many consumers would like to have their privacy, such as shopping manners to be collected.

Another example is applications correlated to the health care in a smart home or hospital. In this scenario, the sensitive information, such as the behavior of patients, needs to be protected. To moderate these privacy issues, a number of technologies have been proposed in current years, such as anonymization, randomly delay, temporary identification, and encryption.

5) Security:

IoT connects more devices together; it offers additional decentralized entry position for malware. Additional layers of software, combination of middleware, APIs, M2M communication, etc. produce more complexity and new security threats. The security troubles become an exceptionally important issue after the data analysis systems find the hidden or perceptive information from the IoT. To secure the information, present encryption technology rented from the WSNs or other networks must be carefully reviewed, when they are used to construct IoT[13]. IoT permits numerous daily things to be tracked, supervised, and associated, and a lot of personal and private information can be collected routinely. For example, the bio-sensor in the food industry can be used to observe hotness and bacterial composition of food stored in the refrigerator. When a quantity of food becomes deteriorated, data can be sent to the food company through the network. However, such data should be kept back severely confidential with the intention of protecting the status of a food company. A consistent security protection mechanism for IoT desires to be researched from the following aspects: 1) the clarity of security and privacy from the views of social, legal, and culture; 2) trust and reputation mechanism; 3) communication security for instance end-to-end encryption; 4) privacy of communication and user data; and 5) security on services and applications.

6) Developing architectures, protocols and competing standards:

The fast development of IoT builds the standardization complicated. Standardization in IoT intend to lower the opening barriers for the new service providers and users, to improve the interoperability of various applications/systems and to permit products or services to perform better at a higher level. A lot of coordination in standardization efforts are required to make sure devices and applications from different countries to be able to share information. A variety of standards used in IoT (e.g., security standards, communication standards, and identification standards) might be the key enablers for the increase of IoT technologies and must be designed to embrace emerging technologies. Specific issues in IoT standardization include interoperability issue, radio access level issues, and semantic interoperability, and security and privacy issues. Industry-specific rules or principles for applying IoT in industrial environments are also optional for easier integration of different services.

IV. APPLICATIONS OF IOT

IoT applications are still in its early step. But the utilization of IoT is quickly emerging and growing. A small number of IoT applications are being introduced and/or installed in a range of industries including ecological screening, healthcare examining, inventory and production management, food supply chain (FSC), transportation, workplace and home maintenance, safety, and supervision.

A. MAJOR APPLICATION AREAS OF IoT

To build a **smart city**, need to implement Smart Parking, Structural health, Noise Urban Maps, Traffic Congestion[33], Smart Lighting, Electromagnetic Field Levels, Waste supervision and smart road facilities. To create a **smart environment,** need to apply Forest Fire Detection, Air Pollution, Snow Level Monitoring, Earthquake Early Detection, Landslide and Avalanche Prevention mechanisms. Security and emergencies plays a major role in all the environments like industry, living places[29], etc., Hence Explosive and Hazardous Gases, Radiation Levels, Liquid Presence, and Perimeter Access Control could be monitored. To utilize a **smart watering** environment, drinkable water

supervision, Water Leakages, River Floods, Chemical leakage detection in rivers, Swimming pool remote measurement, Pollution levels in the sea, Water Leakages, River Floods could be done using sensors[16]. For the effective usage of various energy resources, **smart metering** can be maintained through Smart Grid, Tank Level, Photovoltaic Installations, Water Flow, Silos Stock Calculation methods. Smartness in **retail** applications is essential to save the money and time for customers and improvement in the business for retailers, so Supply Chain Control, NFC Payment, Intelligent Shopping Application, and Smart Product Management should be maintained. To monitor **manufacturing control**, M2M Applications, interior Air Quality, heat Monitoring, Ozone existence, Indoor spot , Vehicle Auto-diagnosis should be tracked. For **smart agriculture** and **smart animal farming**, it is necessary to monitor Wine Quality Enhancing, Green Houses, Golf Courses, Meteorological Station Network, Compost, Hydroponics, Offspring Care, Animal Tracking, and Toxic Gas Levels. In **eHEALTH monitoring**, Fall Detection, Medical Fridges, Sportsmen Care, Patients Surveillance, Ultraviolet Radiation should be done.

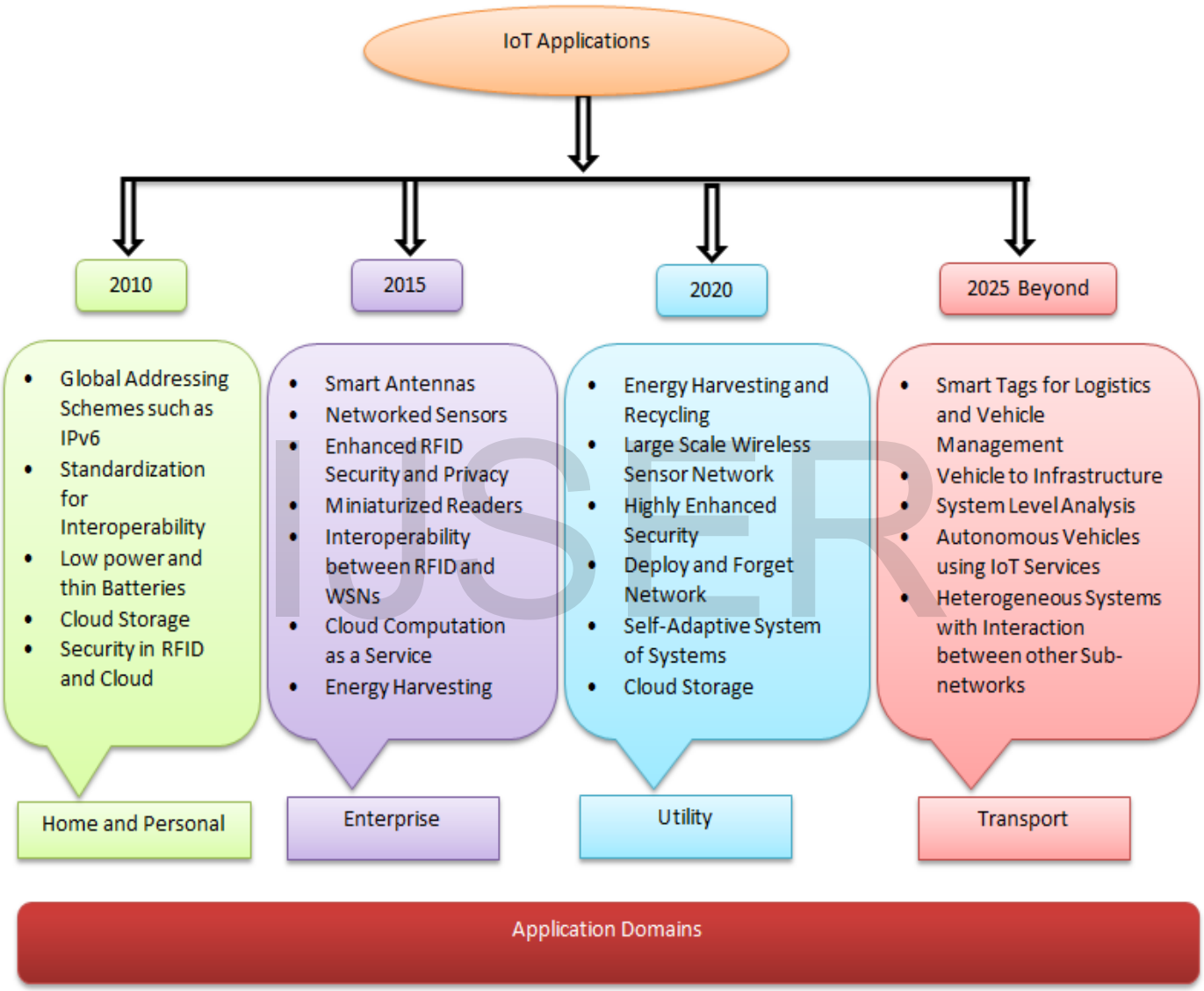

Fig. 3 Applications of IoT

B. *CONTEXT AWARENESS OF IoT*

In order to standardize the communication between various sensors and the implementation of working models in IoT applications like smart-homes and smart-cities, a technique to detain the dynamic growth of the environment in which the IoT devices are immersed is required. In other

words, the challenge is that of defining a structure capable to dynamically change the behavior of the devices on the basis of the situation. This is more related under a cyber-security and privacy perspective as the same device, in different context, it might be essential to respond in a different manner to address the cyber-security requirements imposed. A Context based security and privacy framework for IoT has to provide features to dynamically adapt access rules and information granularity to the situation. In case of emergency, for example, personal information concerning some possible allergy of a patient should be instantly made available to the doctors but to nobody else, even if the patient cannot give explicit approval in that moment. The context switching should be automatically applied by all the IoT devices involved according to specific security and privacy rules as soon as a change in the context is detected or notified .On the other hand, the system should also be able to avoid malicious user to "emulate" crisis scenarios and impersonate doctors in order to be able to access private user information. Another source of problems can be represented by the sensors/actuators employed by the IoT devices to carry out their operations: in normal conditions all the data are collected and processed in a regular way, but for example in a surveillance scenario ,sudden deterioration of the quality of the images (due to different reasons like hardware failures or malicious activities) may stimulate fake consequences of the tasks applied in the framework and hamper the overall decision process in the algorithms used to make sure the system safety and trust.In this case, Data integrity is very essential since both false positives and misdetections can cause severe problems in the scrutiny system. Though, in this case aside from the data integrity, the confidentiality of the data should be ensured in a way that the surveillance video should only be disclosed to the administrator of the system and to the persons that have access privileges and not to anyone else.

The IoT application space is very diverse and IoT applications serve diverse users. Each User categories have dissimilar driving requirements. From the perspective of IoT there are three important user categories: The individual citizens, Community of citizens and enterprises. Some specific needs of the individual citizens/human users for the IoT applications are (1) to enhance their security or the security of their family members –for example remotely controlled alarm systems, or activity detection for aged people, (2) to make it possible to take certain actions in a more suitable manner –for example a personal inventory remainder, (3) to develop the life style and (4) to reduce the cost of living. To deal with the special issues of the whole community, there are three major categories: (1) To protect the environment (2) To create new jobs and ensure existing ones are sustainable and (3) To ensure public security. The third category of IoT, Enterprises have different needs and different drivers to present the IoT based solutions are (1) Increased Productivity (2) Market Differentiation-Able to differentiate from different products (3) Cost Efficiency.

With the large number of IoT devices monitoring the environment, it is almost inevitable that they capture data that can be sensitive to citizens. One of the major enemies of the privacy by design is the reuse of data between applications, because this process allows the link ability of information which is a main privacy threat. Privacy by design is very much related with the context awareness, since one key mechanism to ensure privacy would be to use context information in order to gather from the device only the exact required information that is needed for a specific application and avoid gathering unneeded data that can raise possible privacy threats.

V. CONCLUSION

As a multipart cyber-physical system, IoT integrates a variety of devices operated with sensing, identification, processing, communication, and networking capabilities. Specifically, sensors and actuators are getting progressively more influential, less costly and smaller, which makes their use everywhere. Industries have great attention for setting up IoT devices to expand industrial applications such as automated monitoring, control, management, and maintenance. We primarily initiate the background and architecture model of IoT and later discuss the fundamental challenges that might be faced in IoT. Next, we bring in various key applications of IoT. After that, we studied the some challenges faced while using IoT applications. Different from other IoT survey papers, a main role of this review paper is that it focuses on IoT applications and highlights the challenges for future researchers. Our final goal is to build a foundation that helps to know what has taken place in the IoT marketplace in the earlier period so researchers can plan for the future more competently and effectively.

REFERENCES

[1] Li Da Xu, Wu He, and Shancang Li, "Internet of Things in Industries: A Survey", *IEEE Transactions on Industrial Informatics*, Vol. 10, No. 4, November 2014.

[2] Charith Perera, Chi Harold Liu, Srimal Jayawardena, and Min Chen, "A Survey on Internet of Things from Industrial Market Perspective", *IEEE Access*, January 2015.

[3] Jun Huang, Yu Meng, Xuehong Gong, Yanbing Liu, and Qiang Duan, "A Novel Deployment Scheme for Green Internet of Things", *IEEE Internet of Things Journal*, Vol. 1, No. 2, April 2014.

[4] Huansheng Ning and Hong Liu, Laurence T. Yang, "Cyberentity Security in the Internet of Things", *IEEE Computer Society*, Vol. 1, No. 3, December 2013.

[5] John A. Stankovic, Life Fellow, "Research Directions for the Internet of Things", *IEEE Internet of Things Journal*, Vol. 1, No. 1, February 2014.

[6] Chun-Wei Tsai, Chin-Feng Lai, Ming-Chao Chiang, and Laurence T. Yang, "Data Mining for Internet of Things: A Survey", *IEEE Communications Surveys & Tutorials*, Vol. 16, No. 1, First Quarter 2014.

[7] Vassilis Foteinos, Dimitris, Kelaidonis, George Poulios, Panagiotis Vlacheas, Vera Stavroulaki, and Panagiotis Demestichas, "Cognitive Management for the Internet of Things, A Framework for Enabling Autonomous Applications", *IEEE vehicular technology magazine*, December 2013.

[8] Alexander Gluhak, Srdjan Krco, Michele Nati, Dennis Pfisterer, Nathalie Mitton and Tahiry Razafindralambo, "A Survey on Facilities for Experimental Internet of Things Research", *IEEE Communications Magazine*, November 2011.

[9] Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi, "Internet of Things for Smart Cities", *IEEE Internet of Things Journal*, Vol. 1, No. 1, February 2014.

[10] Sye Loong Keoh, Sandeep S. Kumar, and Hannes Tschofenig, "Securing the Internet of Things: A Standardization Perspective", *IEEE Internet of Things Journal*, Vol. 1, No. 3, June 2014.

[11] Antonio M. Ortiz, Dina Hussein, Soochang Park, Son N. Han, and Noel Crespi, "The Cluster between Internet of Things and Social Networks: Review and Research Challenges", *IEEE Internet of Things Journal*, Vol. 1, No. 3, June 2014.

[12] Pin-Yu Chen, Shin-Ming Cheng, and Kwang-Cheng Chen, "Information Fusion to Defend Intentional Attack in Internet of Things", *IEEE Internet of Things Journal*, Vol. 1, No. 4, August 2014.

[13] Michele Nitti, Roberto Girau, and Luigi Atzori, "Trustworthiness Management in the Social Internet of Things*", IEEE Transactions on Knowledge and Data Engineering*, Vol. 26, No. 5, May 2014.

[14] Burak Kantarci, and Hussein T. Mouftah, "Trustworthy Sensing for Public Safety in Cloud-Centric Internet of Things", *IEEE Internet of Things Journal*, Vol. 1, No. 4, August 2014.

[15] Al-kindy Athman Abdalla and Al-Sakib Khan Pathan, "On Protecting Data Storage in Mobile Cloud Computing Paradigm", Jan-Feb 2014.

[16] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[17] J. Zheng, D. Simplot-Ryl, C. Bisdikian, and H. Mouftah, "The Internet of Things," *IEEE Commun. Mag*., vol. 49, no. 11, pp. 30–31, Nov. 2011.

[18] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, "From today's Intranet of Things to a future Internet of Things: A wireless-and mobility-related view," *IEEE Wireless Commun.*, vol. 17, no. 6, pp. 44–51, Dec. 2010.

[19] D. Uckelmann, M. Harrison, and F. Michahelles, "An architectural approach towards the future Internet of Things," in Architecting *the Internet of Things. Berlin, Germany: Springer-Verlag*, 2011, pp. 1–24.

[20] A. Bassi and G. Horn," Internet of Things in 2020: A Roadmap for the Future", *Brussels, Belgium: Eur. Comm.: Inform. Soc. Media*, 2008.

[21] K. Ashton, That ''Internet of Things'', *RFiD Journal*, 2009.

[22] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, "Vision and challenges for realising the Internet of Things", *Cluster of European Research Projects on the Internet of Things—CERP IoT*, 2010.

[23] J. Buckley (Ed.), "The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems", *Auerbach Publications*, New York, 2006.

[24] Murad Khan and Kijun Han, "A Review of Handover Techniques in Wireless Ad hoc Networks Based on IEEE 802.21 Media Independent Handover Standard", Sep-Oct 2014.

[25] J. Belissent, "Getting clever about smart cities: new opportunities require new business models", *Forrester Research*, 2010.

[26] E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, et al., "Building the Internet of Things using RFID The RFID ecosystem experience", *IEEE Internet Computing*, pp. 48–55, 2009.

[27] M. Zorzi, A. Gluhak, S. Lange, "A. Basis, From today's Intranet of Things to a future Internet of Things: a wireless- and mobility-related view", *IEEE Wireless Communications*, pp. 43–51, 2010.

[28] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, T. Razafindralambo, "A survey on facilities for experimental Internet of Things research", *IEEE Communications Magazine*, pp. 58–67, 2011.

[29] M. Darianian, M.P. Michael, "Smart home mobile RFID-based Internet-of- Things systems and services", *International Conference on Advanced Computer Theory and Engineering*, pp. 116–120, 2008.

[30] H.S. Ning, Z.O. Wang, "Future Internet of Things architecture: like mankind neural system or social organization framework", *IEEE Communications Letters*, pp. 461–463, 2011.

[31] L. Atzori, A. Iera, G. Morabito, "SIoT: giving a social structure to the Internet of Things", *IEEE Communications Letters*, pp. 1193–1195, 2011.

[32] X. Li, R.X. Lu, X.H. Liang, X.M. Shen, J.M. Chen, X.D. Lin, "Smart community: an Internet of Things application", *IEEE Communications Magazine*, pp. 68–75,2011.

[33] M. Zhang, T. Yu, G.F. Zhai, "Smart transport system based on The Internet of Things, *Applied Mechanics and Materials*, pp. 1073–1076, 2011.

[34] M. Yun, B. Yuxin, "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid", *Advances in Energy Engineering*, ICAEE, pp. 69–72, 2010.

[35] I.F. Akyildiz, T. Melodia, K.R. Chowdhury, "A survey on wireless multimedia sensor networks", *Computer Networks*, pp. 921–960, 2007.

[36] T.S. Lopez, D.C. Ranasinghe, M. Harrison, D. McFarlane, "Adding sense to the Internet of Things an architecture framework for smart objective systems", *Pervasive Ubiquitous Computing*, pp. 291–308, 2012.

[37] A.P. Castellani, N. Bui, P. Casari, M. Rossi, Z. Shelby, M. Zorzi, "Architecture and protocols for the Internet of Things: a case study", pp. 678–683, 2010.

[38] A. Katasonov, O. Kaykova, O. Khriyenko, S. Nikitin, and V. Y. Terziyan,"Smart semantic middleware for the Internet of Things," *ICINCO-ICSO*, vol. 8, pp. 169–178, 2008.

[39] M. Kranz, P. Holleis, and A. Schmidt, "Embedded interaction: Interacting with the Internet of Things," *IEEE Internet Comput.*, vol. 14, no. 2, pp. 46–53, Mar./Apr. 2010.

[40] D. Guinard, V. Trifa, S. Karnouskos, P. Spiess, and D. Savio, "Interacting with the SOA-based Internet of Things: Discovery, query, selection, and on-demand provisioning of web services," *IEEE Trans. Services Comput*., vol. 3, no. 3, pp. 223–235, Jul./Sep. 2010.

[41] S. Evdokimov, B. Fabian, S. Kunz, and N. Schoenemann, "Comparison of discovery service architectures for the Internet of Things," in *Proc. IEEE Int. Conf. Sens. Netw. Ubiquitous Trustworthy Comput. (SUTC)*, pp. 237–244, 2010.

S.Prince Sahaya Brighty is currently working as Assistant Professor in the Department of Computer Science and Engineering at Sri Ramakrishna Engineering College, Coimbatore. She has 7.3 years of experience in teaching. Her Research area is Wireless sensor networks and Internet of Things.She has 2 years of teaching experience in CAPE Institute of Technology, Nagercoil . She have guided around 6 UG projects till now. She has presented paper in 2 International and 4 National conferences and she has attended various seminars, workshops and faculty devolpment programme in various institutions. She is a lifetime member of IRACST and IAENG.

Email: brighty.s@srec.ac.in

.P.Selvanayaki,M.E., is currently working as Assistant professor in the Department of Computer Science and Engineering at Sri Ramakrishna Engineering College, Coimbatore. She has a Bachelor of Engineering in Computer Science and Engineering, Master Degree in Network Engineering. Her research and teaching interests include Computer Networks and Internet of Things. She is a Life member of ISTE, IACSIT, IAENG and she has published several research papers in Conferences.

Email: selvanayaki.p@srec.ac.in

M.Kiruthika is currently working as Assistant Professor in the Department of Computer Science and Engineering at Sri Ramakrishna Engineering College, Coimbatore. She holds her Master of Engineering in Computer Science and Engineering from Government College of Technology, Anna University in 2014 and Bachelor of Engineering in Computer Science and Engineering from Dr. Mahalingam College of Engineering and Technology, Anna University in 2012. Her research and teaching interests include Internet of Things, Database Management System and Network Security. She has published a paper in an International Journal, International and National Conference**. Email:** kiruthika.m@srec.ac.in