International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

The Internet of Things: A Survey on Technology and Trends

Shubham Bhatia[1], Abhishek Chauhan[2], Vaibhav K. Nigam[3]

[1] *student, Dept. of Information and technology, JIIT University, sector-62, Noida, UP, INDIA*
[2] *student, Dept. of Electronics and Communication engineering, JIIT University, sector-62, Noida*
[3] *student, Dept. of Information and technology, JIIT University, sector-62, Noida, UP, INDIA*

Abstract - *this survey reports on the current state of research on the Internet of Things (IoT) by reviewing the previous work, identifying the current trends, describing challenges that IoT faces technologically. The Main technique of this concept is the integration of various technologies. In this work, we describe the important technologies involved in the implementation of Internet of Things and the major application area where the Internet of Things will play a significant role. On the latter part we have discussed about the crucial issues which are to be addressed before the worldwide acceptance of these technologies. The review of the literature yielded some important findings that can stimulate and focus the research efforts of scholars.*

Key Words: Internet of Things, RFID, SOA.

1. INTRODUCTION

The definition of the Internet of Things (IoT) still rather fuzzy and subject to debate it may vary from ambient intelligence, ubiquitous computing, pervasive computing, smart cities and recently everywhere. In the international telecommunications union (ITU) publish their first report on IoT. [1] The report adapted a comprehensive and holistic approach by suggesting that the Internet of Things would connect the world objects in both sensory and intelligent manner through combining technological developments in item identification, embedded systems, sensors, wireless networks and others. [2]Originally, the term IoT was first mentioned in 1999 by the founders of original MIT Auto-ID centre. [3] Auto-ID refers to any broad class of identification technologies used in the industry to automate, reduce errors, and increase efficiency. [4] These identification technologies include smart cars, bar code, bio metrics, sensors and voice recognition

The initial vision of the IoT was to connect physical objects, using RFID tags and to uniquely identify those objects using RFID transponders. This mechanism enabled users to identify and track objects as Neil Gershenfeld noted as early as in 2000 that the price of RFID tags would continue to decrease today prices of individual RFID have dropped below 1 cent, making their adoption within diverse business areas not just technically possible but economically feasible. [5]Recently, the concept of IoT has been brought back into the mainstream with a number of well-known companies pushing it's futuristic benefits. But where is the IoT today, in the reality of our day to day lives? In a few industries the IoT is already making a major impact on our very own quality of life and productivity. Connecting and remotely controlling and monitoring devices via ubiquitous cellular and satellite networks combined with more cost effective price points for device hardware is making the IoT very real solution in these companies

1.1 Main Technologies of Internet of Things.

The Internet of things is a technological revolution that represents the future of computing and communications, and its development needs the support from some innovational technologies.

Radio Frequency Identification is seen as one of the pivotal enablers of the Internet of Things. Objects should be identified so that they could be connected. RFID, which use radio waves to identify items, can provide this function [6]. Sometimes RFID has been labelled as a replacement of bar code, but RFID system can do much more than that. In addition to identify items it also can track items in real-time to get important information about their location and status. RFID has already had some valuable applications in retail, health-care, facilities management [7], etc. A mature RFID technology provides a strong support for the Internet of Things. One of the biggest breakthroughs of the Internet of Things is making the physical world and information world together. Sensors play a very important role to bridge the gap between the physical world and information world. Sensors collect data from their environment, generating information raising awareness about context. So the change of their environment can be monitored and the corresponding things can make some responses if needed [8]. Nanotechnology and miniaturization can make embedded intelligence in things themselves which called smart devices. They can process information, self-configure, make decision independently, just until then there will be a real thing-thing communication.

1.2 Trends

From a long perspective, the development trend of the Internet of Things includes three steps: embedded intelligence, connectivity, interaction. Firstly, we have embedded intelligences which can do actions automatically. There already have been many applications, for example: the RFID tag embedded in food can record the information about the food and we can get the information by using a RFID reader; the washing machine controller can make washing machine complete its work automatically; engine controllers and antilock brake controllers for automobiles; inertial guidance system, flight control hardware/software and other integrated systems in aircraft and missiles; artificial arms with semi-functional hands, etc. [9]. Though all of those devices are intelligent, we can see that they only work alone and locally, there's nothing to do with "network". So the next step is making every smart device can be connected. From the smart connected devices viewpoint, smart devices are not smart because they are just endowed with agent capabilities and all the actions are pre-designed by human, they are smart because they are connected. Things can be connected wired or wirelessly. In the Internet of Things wireless connection will to be the main way. Base on the existed infrastructure, there are many ways to connect a thing: RFID, ZigBee, WPAN, WSN, DSL, UMTS, GPRS, WiFi, WiMax, LAN, WAN, 3G, etc. Connect smart things makes interaction possible.

Even though we can connect anything does not mean things can communicate by themselves. So new smart things should be created which can process information, self-configure, self-maintain, self-repair, make independent decision, eventually even play an active role in their own disposal. Things can interact, they exchange information by themselves. So the form of communication will change from human-human to human-thing to thing-thing. As the Internet of Things is application driven, new business applications should be created which can improve the innovation and development of the Internet of Things [11]. Fig.2 shows a rough development trend of the Internet of Things [12].

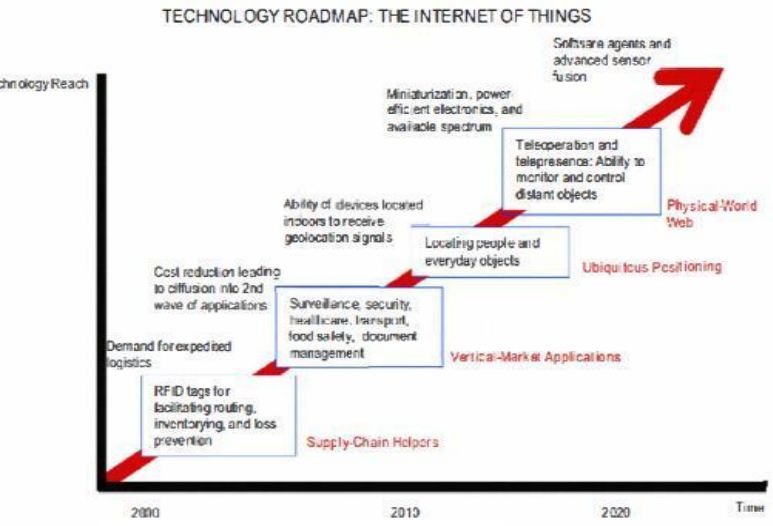

Fig. 1 – Trend of IoT

2. ARCHITECTURE

Current Internet has a five-layered architecture, running with TCP/IP protocols, which has worked well for a long time. However, in the Internet of Things billions of objects are connected which will create much larger traffic and need much more data storages. In addition to these, there still have some other challenges like security, governance, etc. But today's Internet was designed in the 1970s for purposes that bear little resemblance to today's usage scenarios and related traffic patterns. Mismatches between original design and current utilization are now beginning to hamper the Internet's potential. In the BLED Declaration [13] and other supporting statements, they all point out this point. So it is reasonable and essential to design a new architecture for the Internet of Things.

Redesign a new architecture is a very complex project, which needs consider many factors like reliability, scalability, modularity, interoperability, interface, QoS, etc. About the architecture design of the Internet of Things, service-oriented architecture (SOA), exploiting integration with Internet and interfacing with wide ranging edge technologies and associated networks is a key objective.

IoT aims to connect different things over the networks. As a key technology in integrating heterogeneous systems or devices, SOA can be applied to support IoT. SOA has been successfully used in research areas such as cloud computing, WSNs, and vehicular network [17]–[24].

Quite a few ideas have been proposed to create multi-layer SOA architectures for IoT based on the selected technology, business needs, and technical requirements. For example, the International Telecommunication Union recommends that IoT architecture consists of five different layers: sensing, accessing, networking, middleware, and application layers.

2.1 Sensing Layer

IoT can be considered as a world-wide physical interconnected network, in which things can be connected and controlled remotely. As more and more devices are equipped with RFID or intelligent sensors, connecting things becomes much easier [25]. In the sensing layer, the wireless smart systems with tags or sensors are now able to automatically sense and exchange information among different devices. These technology advances significantly improve the capability of IoT to sense and identify things or environment. In some industry sectors, intelligent service deployment schemes and a universal unique identifier (UUID) are assigned to each service or device that may be needed. A device with UUID can be easily identified and retrieved. Thus, UUIDs are critical for successful services deployment in a huge network like IoT [25], [26].

2.2 Networking Layer

The role of networking layer is to connect all things together and allow things to share the information with other connected things. In addition, the networking layer is capable of aggregating information from existing IT infrastructures (e.g., business systems, transportation systems, power grids, healthcare systems, ICT systems, etc.). In SOA-IoT, services provided by things are typically deployed in a heterogeneous network and all related things are brought into the service Internet [14], [27]. This process might involve QoS management and control according to the requirements of users/applications. On the other hand, it is essential for a dynamically changing network to automatically discover and map things in a network. Things need to be automatically assigned with roles to deploy, manage, and schedule the behaviours of things and be able to switch to any other roles at any time as needed. These capabilities enable devices to be able to collaboratively perform tasks. To design the networking layer in IoT, designers need to address issues such as network management technologies for heterogonous networks (such as fixed, wireless, mobile, etc.), energy efficiency in networks, QoS requirements, service discovery and retrieval, data and signal processing, security, and privacy [28].

2.3 Service Layer

Service layer relies on the middleware technology that provides functionalities to seamlessly integrate services and applications in IoT. The middleware technology provides the IoT with a cost-efficient platform, where the hardware and software platforms can be reused. A main activity in the service layer involves the service specifications for middleware, which are being developed by various organizations. A well-designed service layer will be able to identify common application requirements and provide APIs and protocols to support required services, applications, and user needs. This layer also processes all service-oriented issues, including information exchange and storage, data management, search engines, and communication [14], [15], [28]. This layer includes the following components.

1) Service discovery: finding objects that can offer the needed services and information in an efficient way [14].

2) Service composition: enabling the interaction and communication among connected things. The discovery phase leverage the relationships among different things to discover the desired service, and the service composition component is to schedule or re-create more suitable services in order to acquire the most reliable services to meet the request [14], [15].

3) Trustworthiness management: aiming at determining trust and reputation mechanisms that can evaluate and use the information provided by other services to create a trustworthy system [14], [27], [28].

4) Service APIs: supporting the interactions between services required in IoT [16], [28].

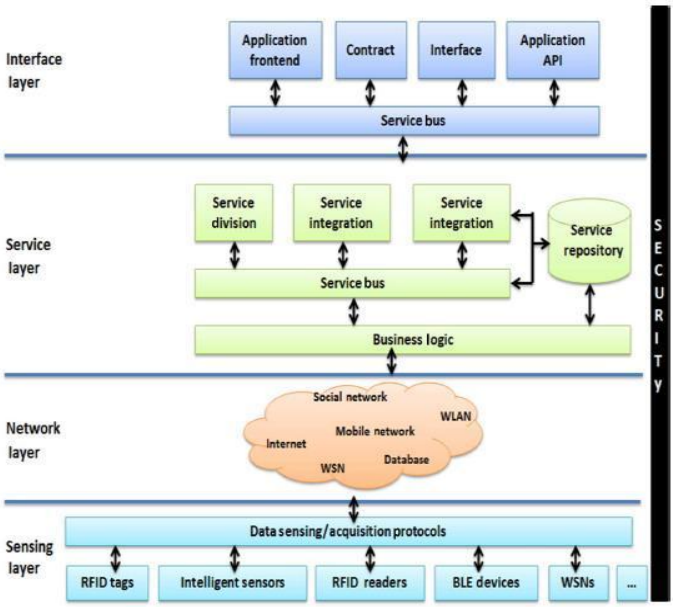

Fig. 2 - SOA for IoT

2.4 Interface Layer

In IoT, a large number of devices involved are made by different manufacturers/vendors and they do not always follow the same standards/protocols. As a result of the heterogeneity, there are many interaction problems with information exchange, communication between things, and cooperative event processing among different things. Furthermore, the constant increase of things participating in an IoT makes it harder to dynamically connect, communicate, disconnect, and operate. There is also a necessity for an interface layer to simplify the management and interconnection of things. An interface profile (IFP) can be seen as a subset of service standards that support interaction with applications deployed on the network. A good interface profile is related to the implementation of Universal Plug and Play (UPnP), which defines a protocol for facilitating interaction with services provided by various things [28], [29]. The interface profiles are used to describe the specifications between applications and services. The services on the service layer run directly on limited network infrastructures in order to effectively find new services for an application, as they connect to the network. Recently, a SOCRADES integration architecture (SIA) has been proposed to effectively interact between applications and services [28], [30]. Traditionally, the service layer provides universal API for applications. However, the recent research results on SOA-IoT reported [31] that service provisioning process (SPP) can also effectively provide interaction between applications and services. The SPP first performs a "types

query" that sends a request for services with a generic WSDL format, and then uses a "candidate search" mechanism to find potential services. Based on the "Application context" and "QoS information," all service instances are ranked and an "On-Demand service provisioning" mechanism will be used to identify a service instance that matches the application's requirements. In the end, a "Process Evaluation" is used to evaluate the process [31], [32].

3. APPLICATION

There are several application domains which will be impacted by the emerging Internet of Things. The applications can be classified based on the type of network availability, coverage, scale, heterogeneity, repeatability, user involvement and impact [34]. We categorize the applications into four application domains:(1) Personal and Home; (2) Enterprise; (3) Utilities; and(4) Mobile. This is depicted in Fig. 3, which represents Personal and Home IoT at the scale of an individual or home, Enterprise IoT at the scale of a community, Utility IoT at a national or regional scale and Mobile IoT which is usually spread across other domains mainly due to the nature of connectivity and scale.

There is a huge crossover in applications and the use of data between domains. For instance, the Personal and Home IoT produces electricity usage data in the house and makes it available to the electricity (utility) company which can in turn optimize the supply and demand in the Utility IoT. The internet enables sharing of data between different service providers in a seamless manner creating multiple business opportunities. A few typical applications in each domain are given.

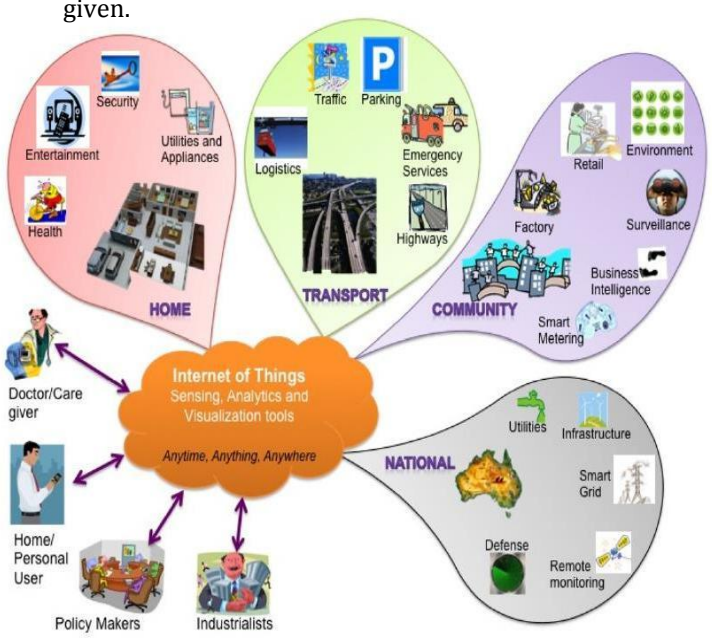

Fig. 3 – IoT schematic showing the end users and application areas based on data.

3.1 Personal and home

The sensor information collected is used only by the individuals who directly own the network. Usually Wi-Fi is used as the backbone enabling higher bandwidth data (video) transfer as well as higher sampling rates (Sound). Ubiquitous healthcare [33] has been envisioned for the past two decades. IoT gives a perfect platform to realize this vision using body area sensors and IoT back end to upload the data to servers. For instance, a Smartphone can be used for communication along with several interfaces like Bluetooth for interfacing sensors measuring physiological parameters. So far, there are several applications available for Apple iOS, Google Android and Windows Phone operating systems that measure various parameters. However, it is yet to be centralized in the cloud for general physicians to access the same.

An extension of the personal body area network is creating a home monitoring system for elderly care, which allows the doctor to monitor patients and the elderly in their homes thereby reducing hospitalization costs through early intervention and treatment [35, 36]. Control of home equipment such as air conditioners, refrigerators, washing machines etc., will allow better home and energy management. This will see consumers become involved in the IoT revolution in the same manner as the Internet revolution itself [37, 38]. Social networking is set to undergo another transformation with billions of interconnected objects [39, 40]. An interesting development will be using a Twitter like concept where individual 'Things' in the house can periodically tweet the readings which can be easily followed from anywhere creating a TweetOT. Although this provides a common framework using cloud for information access, a new security paradigm will be required for this to be fully realized [41].

3.2. Enterprise

We refer to the 'Network of Things' within a work environment as an enterprise based application. Information collected from such networks are used only by the owners and the data may be released selectively. Environmental monitoring is the first common application which is implemented to keep track of the number of occupants and manage the utilities within the building (e.g., HVAC, lighting). Sensors have always been an integral part of the factory setup for security, automation, climate control, etc. This will eventually be replaced by a wireless system giving the flexibility to make changes to the setup whenever required. This is nothing but an IoT subnet dedicated to factory maintenance. One of the major IoT application areas that is already drawing attention is Smart Environment IoT [34, 41]. There are several testbeds being implemented and many more planned in the coming years. Smart environment includes subsystems as shown in Table 1 and the

characteristics from a technological perspective are listed briefly. It should be noted that each of the sub domains cover many focus groups and the data will be shared. The applications or use-cases within the urban environment that can benefit from the realization of a smart city WSN capability are shown in Table 2. These applications are grouped according to their impact areas. This includes the effect on citizens considering health and well-being issues; transport in light of its impact on mobility, productivity, pollution; and services in terms of critical community services managed and provided by local government to city inhabitants.

Table 1
Smart environment application domains.

	Smart home/office	Smart retail	Smart city	Smart agriculture/forest	Smart water	Smart transportation
Network size	Small	Small	Medium	Medium/large	Large	Large
Users	Very few, family members	Few, community level	Many, policy makers, general public	Few, landowners, policy makers	Few, government	Large, general public
Energy	Rechargeable battery	Rechargeable battery	Rechargeable battery, energy harvesting	Energy harvesting	Energy harvesting	Rechargeable battery, Energy harvesting
Internet connectivity	Wifi, 3G, 4G LTE backbone	Wifi, 3G, 4G LTE backbone	Wifi, 3G, 4G LTE backbone	Wifi, satellite communication	Satellite communication, microwave links	Wifi, satellite communication
Data management	Local server	Local server	Shared server	Local server, shared server	Shared server	Shared server
IoT devices	RFID, WSN	RFID, WSN	RFID, WSN	WSN	Single sensors	RFID, WSN, single sensors
Bandwidth requirement	Small	Small	Large	Medium	Medium	Medium/large
Example testbeds	Aware home [29]	SAP future retail center [30]	Smart Santander [31], citySense [32]	SiSViA [33]	GBROOS [34], SEMAT [35]	A few trial implementations [36,37]

Table 2
Potential IoT applications identified by different focus groups of the city of Melbourne.

Citizens	
Healthcare	Triage, patient monitoring, personnel monitoring, disease spread modeling and containment—real-time health status and predictive information to assist practitioners in the field, or policy decisions in pandemic scenarios
Emergency services, defense	Remote personnel monitoring (health, location); resource management and distribution, response planning; sensors built into building infrastructure to guide first responders in emergencies or disaster scenarios
Crowd monitoring	Crowd flow monitoring for emergency management; efficient use of public and retail spaces; workflow in commercial environments
Transport	
Traffic management	Intelligent transportation through real-time traffic information and path optimization
Infrastructure monitoring	Sensors built into infrastructure to monitor structural fatigue and other maintenance; accident monitoring for incident management and emergency response coordination
Services	
Water	Water quality, leakage, usage, distribution, waste management
Building management	Temperature, humidity control, activity monitoring for energy usage management, D heating, Ventilation and Air Conditioning (HVAC)
Environment	Air pollution, noise monitoring, waterways, industry monitoring

3.3 Utilities

The information from the networks in this application domain is usually for service optimization rather than consumer consumption. It is already being used by utility companies (smart meter by electricity supply companies) for resource management in order to optimize cost vs. profit. These are made up of very extensive networks (usually laid out by large organization on a regional and national scale) for monitoring critical utilities and efficient resource management. The backbone network used can vary between cellular, Wi-Fi and satellite communication. Smart grid and smart metering is another potential IoT application which is being implemented around the world [43]. Efficient energy consumption can be achieved by continuously monitoring every electricity point within a house and using this information to modify the way electricity is consumed. This information at the city scale is used for maintaining the load balance within the grid ensuring high quality of service. Video based IoT [44], which integrates image processing, computer vision and networking frameworks, will help develop a new challenging scientific research area at the intersection of video, infrared, microphone and network technologies. Surveillance, the most widely used camera network applications, helps track targets, identify suspicious activities, detect left luggage and monitor unauthorized access. Automatic behaviour analysis and event detection (as part of sophisticated video analytics) is in its infancy and breakthroughs are expected in the next decade as pointed out in the 2012 Gartner Chart (refer Fig. 4).

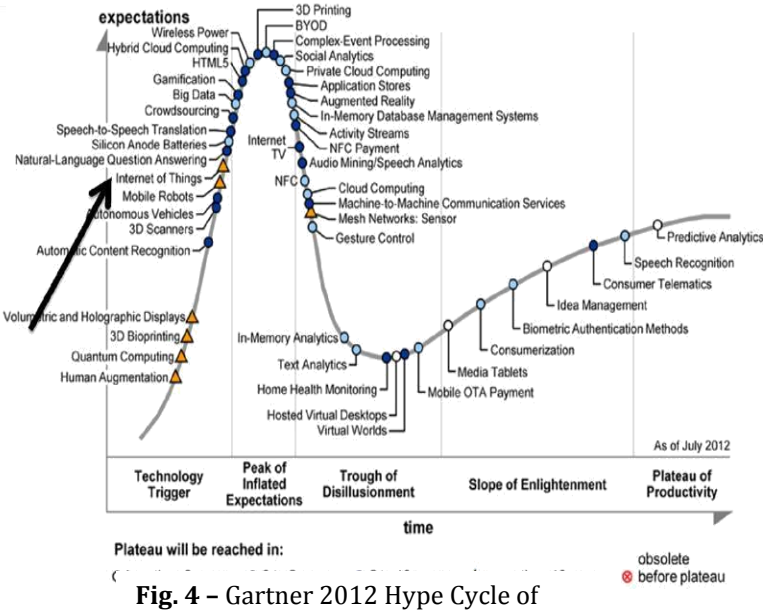

Fig. 4 – Gartner 2012 Hype Cycle of emerging technologies, [10]

drinking water is another critical application that is being addressed using IoT. Sensors measuring critical water parameters are installed at important locations in order to ensure high supply quality. This avoids accidental contamination among storm water drains, drinking water and sewage disposal. The same network can be extended to monitor irrigation in agricultural land. The network is also extended for monitoring soil parameters which allows informed decision making concerning agriculture [45].

3.4 Mobile

Smart transportation and smart logistics are placed in a separate domain due to the nature of data sharing and backbone implementation required. Urban traffic is the main contributor to traffic noise pollution and a major contributor to urban air quality degradation and greenhouse gas emissions. Traffic congestion directly imposes significant costs on economic and social activities in most cities. Supply chain efficiencies and productivity, including just-in-time operations, are severely impacted by this congestion causing freight delays and delivery schedule failures. Dynamic traffic information will affect freight movement, allow better

planning and improved scheduling. The transport IoT will enable the use of large scale WSNs for online monitoring of travel times, origin– destination (O–D) route choice behavior, queue lengths and air pollutant and noise emissions. The IoT is likely to replace the traffic information provided by the existing sensor networks of inductive loop vehicle detectors employed at the intersections of existing traffic control systems.

They will also underpin the development of scenario-based models for the planning and design of mitigation and alleviation plans, as well as improved algorithms for urban traffic control, including multi-objective control systems. Combined with information gathered from the urban traffic control system, valid and relevant information on traffic conditions can be presented to travelers [46]. The prevalence of Bluetooth technology (BT) devices reflects the current IoT penetration in a number of digital products such as mobile phones, car hands-free sets, navigation systems, etc. BT devices emit signals with a unique Media Access Identification (MAC-ID) number that can be read by BT sensors within the coverage area. Readers placed at different locations can be used to identify the movement of the devices. Complemented by other data sources such as traffic signals, or bus GPS, research problems that can be addressed include vehicle travel time on motorways and arterial streets, dynamic (time dependent) O–D matrices on the network, identification of critical intersections, and accurate and reliable real time transport network state information [42]. There are many privacy concerns by such usages and digital forgetting is an emerging domain of research in IoT where privacy is a concern [47]. Another important application in mobile IoT domain is efficient logistics management [42]. This includes monitoring the items being transported as well as efficient transportation planning. The monitoring of items is carried out more locally, say, within a truck replicating enterprise domain but transport planning is carried out using a large scale IoT network.

4. CHALLENGES

The first issue to consider is how objects will join the internet. There are two ways for a typical computing device to connect to the Internet: (1) independently using a mobile broadband connection to an Internet Service Provider (ISP). Two popular examples are a laptop equipped with a mobile broadband modem and a mobile device that connect to the internet via 3G that has an inbuilt modem; and (2) via a local-area wireless or wired network which is connected to a base station or a router. Examples are local area networks (LANs) that connect computers and devices, within the same geographical area together. Each device on the network is regarded as a node with one of them designated as a gateway. A gateway computing device, for instance, acts as a router, sharing Internet connection to other nodes.

For the realization of both (1) and (2), these devices rely on a communication protocol for exchanging information over a network; normally the TCP/IP protocol suite. These devices are uniquely identified (via IP or MAC) by the communication protocols. However in the IoT, objects need to be identified uniquely by IoT applications on the Internet. This opens the door for numerous issues such as identifying objects, name space, object addressing and the need for a global unique ID.

4.1 Object Naming

Currently, DNS is the Internet naming service that translates the IP addresses into human friendly host names. Object name service is among the essential and key elements in the IoT that need to be researched. The IoT will include a large number of objects which are considered on the network as nodes, each of which will produce contents that should be retrievable by authorized users or objects. This requires effective object addressing or naming policies. Additionally, the characteristics of the traffic exchanged by smart objects, in the IoT, remain unknown at least for now. Further contributions are required to determine if the TCP protocol is adequate to use in the IoT or if a new concept of a transport layer is required. This is due to the fact that the TCP protocol is connection-oriented, by which a communication session starts with a connection setup procedure known as the three handshake. Given that some of the communications within the IoT will involve the exchange of only small amount of data generated from constrained devices, the TCP protocol cannot be used efficiently for transmission control. For example, if the amount of data, generated by an object, to be exchanged in a single session is very small, the TCP congestion control is considered to be ineffective, given that the whole TCP session will be concluded with the transmission of the first segment and the consequent reception of the corresponding acknowledgement message [48].

4.2 Interoperability

In typical computing environments, computing devices are treated equally when they are connected to the Internet. Their functionalities vary depending on how users use them. However, in the IoT, each object would be subject to different conditions such as power availability and communication bandwidth requirements. In addition, objects on the IoT might be made by different manufacturers that do not necessarily comply with the same standards.

This difference results in heterogeneous devices that might not be able to communicate directly with each other, raising integration issues. Service description, common practices, standards and discovery mechanisms should be interoperable to allow interactions between different objects

4.3 Identify Management

Identity management systems have been already identified by previous researchers, for instance see [49], as an essential component in the successful operation of the IoT. In the recent years, many frameworks for identity management have been developed, e.g. Open ID. OpenID describes how users can be authenticated in a decentralized manner. This decentralized technique allows users to process their digital identities quickly and reliably. Also, it eliminates the need of deploying independent ad-hoc identity management systems by the service provider. In any of these authentication processes, there is a need of preserving users' privacy in the IoT where most of the entities may be untrusted.

5. ISSUES

5.1 Addressing and Networking Issues

Each and every device connected in the network has a unique address by which it can be identified. As the IoT is gaining grounds in scenario, the demand for these unique address increases at a very fast rate. There are very limited number of address available in IPv4 addressing and will soon reach zero as it identifies each node through a 4-byte address. To handle the ever increasing demand of unique address, one require IPv6 addressing scheme to fulfill the requirement. IPv6 addresses are expressed by means of 128 bits and, therefore, it is possible to define 1038 addresses, which should be enough to identify any object.

Another important issue is regarding networking i.e. which protocol is to be used to send the data from source to destination. In traditional internet, the protocol utilized at the transport layer for reliable communications is the Transmission Control Protocol (TCP). It is clear that TCP is insufficient for the IoT because we need to set-up a connection first in case of TCP, but most of communication in IoT is a very short communication. So, considerable time will be wasted in the connection setup. One more issue with TCP is congestion control, TCP is responsible for end-to-end congestion control, but in case of IoT the amount of data transfer is very small, so TCP congestion control is useless.

As a consequence, TCP cannot be used efficiently for the end-to-end transmission control in the IoT. Till now, no solutions have been proposed and, therefore, research is required in this area.

5.2 Privacy and Security Issues

The IoT is extremely vulnerable to attacks as its components spend most of the time unattended, so it became very easy to attack them. Apart from this, one more thing is that, most of the communication is wireless which makes snooping very easy. The major problems related to security concern authentication and data integrity. Authentication is required before making a connection between the two devices to prevent data theft. The infrastructure is required for the authentication as we generally have to exchange some public and private keys through the node. Solutions like cryptography and key management have been proposed in the recent past, but none of them will prevent from the man-in-the-middle attack and proxy attack problem.

5.3 Congestion Issues

Congestion is occurred due to simultaneous messages from several devices that can lead to peak load situation and may have a tremendous impact on the network (3GPP, 2010). This affects the performance of the network, and may lead to failure of the network if the network is overloaded. The congestion situation also occurred because of malfunction of server or application; so to avoid this one has to design an application in such a way that can handle maximum load with minimum failure.

5.4 Data Cleaning Issues

The data cleaning in IoT technology may be required for a variety of reasons:
A. When data is collected from conventional sensors, it may be noisy incomplete or may require probabilistic uncertain modeling.
B. RFID data is extremely noisy incomplete and redundant because a large fraction of the readings are dropped and there are cross reads from multiple sensor readers.

6. CONCLUSION

With the rapid advancement of technology, the Internet of Things (IoT) is no longer seen as a vision of the future. It is becoming a reality in the present. The IoT is expanding the boundaries of the Internet we know today, by enabling a new form of interaction and communication between objects, leading to the vision of "anytime, anywhere, anyone, and anything" communications. This intercommunication results in autonomous exchange of information between object-to object and person-to-object. In this paper, we survey the state-of-art on the IoT, including the manifold definitions, enabling technologies and the major challenging issues. Future works will address these security concerns, specifically, those challenging the location data privacy, safety, governance and trust.

REFERENCES

[1] (2005, *The Internet of Things*. Available: http://www.itu.int/osg/spu/publications/internetofthings/

[2] ITU, "Global Standards for the Internet of Things," ed: ITU, 2012.

[3] K. Ashton, "That 'Internet of Things' Thing," *RFID Journal,* 22 July 2009.

[4] G. Santucci, "The internet of things: Between the revolution of the internet and the metamorphosis of objects," *Harald Sundmaeker, Patrick Guillemin, Peter Friess, Sylvie Woelfflé Vision and Challenges for Realising the Internet of Things.. Cluster of European Research Projects on the Internet of Things (CERPIoT),* 2010.

[5] G. Neil, *when things start to think*: Holt Paperbacks, 2000.

[6] Yuh-Jzer Joung,"RFID and the Internet of Things", Taiwan University, 2007

[7] Christine Legner, Frederic Thiesse, "RFID-Based Maintenance at Frankfurt Airport", IEEE Distributed Systems

[8] Margery Conner," Sensors empower the ' Internet of Things'", 2010

[9] DLJorge Pereira, "From Autonomous to Cooperative Distributed Monitoring and Control: Towards the Internet of Smart Things", 2008

[10] Gartner's hype cycle special report for 2011, Gartner Inc., 2012. http://www.gartner.com/technology/research/hype-cycles/.

[11] Internet Industrial Alliance, GEl, "The Internet of Things industrial development research", 2010

[12] www.wikipedia.com

[13] The BLED Future Internet Declaration, 2008

[14] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Comput. Netw. vol. 54, no. 15, pp. 2787–2805, 2010.

[15] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Netw., vol. 10, no. 7, pp. 1497–1516, 2012.

[16] H. Zhang and L. Zhu, "Internet of things: Key technology, architecture and challenging problems," in Proc. 2011 IEEE Int. Conf. Comput. Sci. Autom. Eng. (CSAE), Shanghai, China, Jun. 10–12, pp. 507–512.

[17] S. Wang, L. Li, K. Wang, and J. Jones, "E-business system integration: A systems perspective," Inf. Technol. Manage., vol. 13, no. 4, pp. 233–249, 2012.

[18] F. Tao, H. Guo, L. Zhang, and Y. Cheng, "Modelling of combinable relationship-based composition service network and the theoretical proof of its scale-free characteristics," Enterp. Inf. Syst., vol. 6, no. 4, pp. 373–404, 2012.

[19] L. Xu, W. Viriyasitavat, P. Ruchikachorn, and A. Martin, "Using propositional logic for requirements verification of service workflow," IEEE Trans. Ind. Informat., vol. 8, no. 3, pp. 639–646, Aug. 2012.

[20] D. Paulraj, S. Swamynathan, and M. Madhaiyan, "Process model-based atomic service discovery and composition of composite semantic web services using web ontology language for services," Enterp. Inf. Syst., vol. 6, no. 4, pp. 445–471, 2012.

[21] H. Panetto and J. Cecil, "Information systems for enterprise integration, interoperability and networking: Theory and applications," Enterp. Inf. Syst., vol. 7, no. 1, pp. 1–6, 2013.

[22] W. Viriyasitavat, L. Xu, and A. Martin, "SWSpec, service workflow requirements specification language: The formal requirements specification in service workflow environments," IEEE Trans. Ind. Informat., vol. 8, no. 3, pp. 631–638, Aug. 2012.

[23] S. Hachani, L. Gzara, and H. Verjus, "A service-oriented approach for flexible process support within enterprises: An application on PLM systems," Enterp. Inf. Syst., vol. 7, no. 1, pp. 79–99, 2013.

[24] L. Xu, "Enterprise Systems: State-of-the-art and future trends," IEEE Trans. Ind. Informat., vol. 7, no. 4, pp. 630–640, Nov. 2011.

[25] Y. Wu, Q. Z. Sheng, and S. Zeadally, "RFID: Opportunities and challenges," in Next-Generation Wireless Technologies, N. Chilamkurti, Ed. New York, NY, USA: Springer, 2013, ch. 7, pp. 105–129.

[26] E. Ilie-Zudor, Z. Kemeny, F. van Blommestein, L. Monostori, and A. van der Meulen, "A survey of applications and requirements of unique identification

systems and RFID techniques," Comput. Ind., vol. 62, no. 3, pp. 227–252, 2011.

[27] C. Han, J. M. Jornet, E. Fadel, and I. F. Akyildiz, "A cross-layer communication module for the internet of things," Comput. Netw., vol. 57, no. 3, pp. 622–633, 2013.

[28] D. Guinard, V. Trifa, S. Karnouskos, P. Spiess, and D. Savio, "Interacting with the soa-based internet of things: Discovery, query, selection, and ondemand provisioning of web services," IEEE Trans. Serv. Comput., vol. 3, no. 3, pp. 223–235, Jul./Sep. 2010.

[29] K. Gama, L. Touseau, and D. Donsez, "Combining heterogeneous service technologies for building an internet of things middleware," Comput. Commun., vol. 35, no. 4, pp. 405–417, 2012.

[30] D. Romero, G. Hermosillo, A. Taherkordi, R. Nzekwa, R. Rouvoy, and F. Eliassen, "RESTful integration of heterogeneous devices in pervasive environments," in Distributed Applications and Interoperable Systems. Berlin, Germany: Springer-Verlag, 2010, ch. 01, pp. 1–4.

[31] H. Zhou, The Internet of Things in the Cloud: A Middleware Perspective. Boca Raton, FL, USA: CRC Press, 2012.

[32] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (SIoT)-when social networks meet the internet of things: Concept, architecture and network characterization," Comput. Netw., vol. 56, no. 16, pp. 3594–3608, 2012.

[33] L. Atzori, A. Iera, G. Morabito, The Internet of Things: a survey, Computer Networks 54 (2010) 2787–2805.

[34] 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 49 (2011) 58–67.

[35] L. Haiyan, C. Song, W. Dalei, N. Stergiou, S. Ka-Chun, A remote markerless human gait tracking for e-healthcare based on content-aware wireless multimedia communications, IEEE Wireless Communications 17 (2010) 44–50.

[36] G. Nussbaum, People with disabilities: assistive homes and environments, in: Computers Helping People with Special Needs, 2006.

[37] A. Alkar, U. Buhur, An Internet based wireless home automation system for multifunctional devices, IEEE Transactions on Consumer Electronics 51 (2005) 1169–1174.

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

[39] H.S. Ning, Z.O. Wang, Future Internet of Things architecture: like mankind neural system or social organization framework IEEE Communications Letters 15 (2011) 461–463.

[40] L. Atzori, A. Iera, G. Morabito, SIoT: giving a social structure to the Internet of Things, IEEE Communications Letters 15 (2011) 1193–1195.

[41] 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 49 (2011) 68–75.

[42] H. Lin, R. Zito, M. Taylor, A review of travel-time prediction in transport and logistics, Proceedings of the Eastern Asia Society for Transportation Studies 5 (2005) 1433–1448.

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

[44] I.F. Akyildiz, T. Melodia, K.R. Chowdhury, A survey on wireless multimedia sensor networks, Computer Networks 51 (2007) 921–960.

[45] H. Jun-Wei, Y. Shouyi, L. Leibo, Z. Zhen, W. Shaojun, A crop monitoring system based on wireless sensor network, Procedia Environmental Sciences 11 (2011) 558–565.

[46] P. Kumar, S. Ranganath, W. Huang, K. Sengupta, Framework for real-time behavior interpretation from traffic video, IEEE Transactions on Intelligent Transportation Systems 6 (2005) 43–53.

[47] V. Mayer-Schönberger, Failing to forget the ''Drunken Pirate'', in: Delete: the Virtue of Forgetting in the Digital Age (New in Paper), first ed., Princeton University Press, 2011, pp. 3–15.

[48] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks,* vol. 54, pp. 2787-2805, 2010.

[49] A. Cavoukian and F. Carter, *7 laws of identity: The case for privacy-embedded laws of identity in the digital age*: Information and Privacy Commissioner of Ontario, 2006.