On the Research and Development of Social Internet of Things

B.K. Tripathy, Deboleena Dutta and Chido Tazivazvino

Abstract The Internet of Things (IoT) has been a new trend in the IT business and the assembling group for quite a while. Yet, in this way, the battle with IoT is that it is attempting to locate an extraordinary advertising message about how it will specifically enhance human lives. It has been stated that the ones who are tied in a social network can give significantly give more exact responses to complicated issues than an individual alone. This rule has been seriously considered in different websites. Lately, with the help of IoT frameworks, it was made possible to connect billions of objects in a very short term. The Social Internet of Things (SIoT) is characterized as an IoT where things are fit for building social associations with different items, independently regarding people. In this chapter we propose to discuss on the origin, development and current status of SIoT and propose some scope for future studies.

1 Introduction

In the year 1832, an electromagnetic broadcast was made by Baron Schilling in Russia; in 1833 Carl Friedrich Gauss and Wilhelm Weber created their own code to convey over a separation of 1200 m inside Gottingen, Germany. In 1950, Alan Turing had stated in his article 'Computing Machinery and Intelligence', "*…It can also be maintained that it is best to provide the machine with the best sense organs that money can buy, and then teach it to understand and speak English. This*

B.K. Tripathy (✉) · D. Dutta · C. Tazivazvino
School of Computing Science and Engineering, VIT University, Vellore 632014, Tamil Nadu, India
e-mail: tripathybk@vit.ac.in

D. Dutta
e-mail: debol.dutta2014@vit.ac.in

C. Tazivazvino
e-mail: chido.sabinaazvino2014@vit.ac.in

C.X. Mavromoustakis et al. (eds.), *Internet of Things (IoT) in 5G Mobile Technologies*, Modeling and Optimization in Science and Technologies 8,
DOI 10.1007/978-3-319-30913-2_8

process could follow the normal teaching of a child". In the year 1969, Arpanet was invented and in 1974 TCP/IP. In the year 1989 World Wide Web was proposed by Tim Berners Lee and he created the first web page in 1991. In 1990 John Romkey had invented a toaster which worked using the TCP/IP. The idea of the Internet of Things first got to be well known in 1999, when MIT Aston Kevin coined the term as "Internet of Things" [1, 2].

When we consider communication, we have always tried and developed the interaction between human to human by sending and receiving data (or information) using different modes and mediums. In the present world, this communication has been in the form of Internet or World Wide Web (abbreviated as 'www'), which if looked closely is again between human and/to human. To break this human and/to human communication, not in a distant future, we can connect human to objects, objects to human and objects to objects; every objects can be connected to each other and more. These networks of devices (or objects) which can connect directly with each other to capture and share vital data can be defined as 'Internet of things (IoT)'. Typically, Internet of Things use the secure service layer (SSL) that connects to a central command and control server in the cloud [3].

The Internet of Things promises to be a source of great benefits to our lives but it definitely will be a source of difficulty for designers of telecommunication networks and applications unless appropriate new communication paradigms are identified. The IoT has been a new trend in the IT business and the assembling group for quite a while. Yet, in this way, the battle with IoT is that it is attempting to locate an extraordinary advertising message about how it will specifically enhance human lives. The IoT vision can be completely accomplished just if items have the capacity to coordinate in an open way. We strongly believe that what will definitely meet the needs of users, designers, and developers is a social approach to the Internet of Things. It has been stated that the ones who are tied in a social network can give significantly give more exact responses to complicated issues than an individual alone. This rule has been seriously considered in different websites. Lately, with the help of IoT frameworks, it was made possible to connect billions of objects in a very short term.

The Social Internet of Things (SIoT) is characterized as an IoT where things are fit for building social associations with different items, independently regarding people. Thusly, an informal organization of articles is made. The objectives being pursued by the SIoT paradigm are clear: to keep separate the two levels of people and things; to allow objects to have their own social networks; to allow humans to impose rules to protect their privacy and only access the result of autonomous inter-object interactions occurring on the objects' social network.

In our vision smart objects (even though extremely intelligent) will not make a difference, but social objects will make it [4].

2 From IoT to SIoT

Now, that we have an idea about the IoT, till now the objects could see and listen to each other, by Socializing the Internet of Things, these objects can talk. Soon we can see business cards with tags which when scanned by a smartphone can direct the person to the website or a YouTube video or a voice navigating to the contact's address with the help of GPS. Much more can be done using the SIoT. Due the upcoming companies and the ideas, there are many individuals, companies or organizations but more than that there are applications. With the help of these applications and interacting objects we can know a new world which would be unexpectedly interesting; eventually much closer than expected [5] (Fig. 1).

SIoT is a network based idea which work on 'relationships' such as *friends* [6]. The objects in a distributed network of SIoT are the nodes which store the information and the data. Each node is a friend to another node or object. To maintain the friendship, the communication is developed with each friend maintains the information and manages the same. Although, every object do not promote themselves as a friend, it requires trust, scalability and interoperability to decide which object is to be promoted as a friend and that is how a system's compatibility and complexities are calculated to maintain a healthy and efficient performance. These require tools, functions for searching the shortest path and computational theory to transfer data providing security at the same time. Using these ideas, SIoT has been developed where the sensors are made smart to detect the objects around and communicate with each other automatically; thus establish a 'friendship'.

Previously, communication was very difficult between people, who stayed far away from each other. It required days and weeks to communicate when birds or human messengers used to travel and deliver the information from one person to another. Later, this communication was simplified with the invention of vehicles, telegram, telegraph and telephone; communication was made quickly both far and near. With the invention of computer, communication now was through cables. This invention was later combined with telephone lines to form a network using a

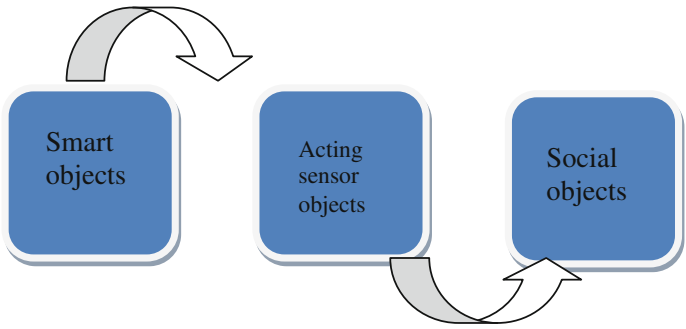

Fig. 1 From smart to socializing objects [4]

modem and thus the internet evolved as a great revolution turning the globe into a network connecting people from one place to another, far and near [7].

Radio Frequency Identification (RFID) is a wireless device. It uses the electromagnetic fields to automatically identify and detect tags to transfer data. These tags are generally attached to the objects and contain the information stored electronically. Mostly used to track the devices, for example track and get the status of the vehicles in toll gates. RFID is considered a pre-requisite for Internet of Things. The concept of Internet of Things, incepted at the Auto-ID (for Automatic Identification) Center of MIT where Sanjay Sharma, David Brock and Aston Kevin used the RFID tags t turn it into a network by connecting the objects to the Internet to create a wireless sensor network. Later, Kevin Aston, executive director of Auto-ID centre, MIT, coined the term "Internet of Things" in the RFID journal [1, 2, 7].

RFID frameworks comprises of a receiving wire and a device, which read the radio recurrence and exchange the data to a transponder, device which can be processed and a tag, which has the RF hardware and data to be transmitted contained in an integrated circuit. RFID frameworks can be utilized pretty much anyplace; tags can be used in rockets to garments from food to pet- anyplace where unique ID system is required. RFID works like bar code that can interact with a framework to track each item that you put in your shopping basket. Let us imagine, one day we go to the supermarket, collect all the items in the display in our basket as per our requirement and then leave the market immediately without standing in the queue for payment. Don't have to wait for anyone to take each item from our basket, scan the bar code and generate the bill. Rather, these RFID will correspond with an electronic sensor, that can be attached to the basket picked up from the supermarket for collecting items or it can be attached to the door of the supermarket that will scan and identify each item in the basket right away. This sensor will send the details to the retailer and to the buyers. The billing detail amount can be sent directly the registered bank of the customer for payment. Thus the amount can be deducted. No lines, no scanning of each item, no time wasted in waiting. The RFID tag can convey data and information for any day to day life from simple to complex tasks, as basic as the details of the owner of a pet, his address to phone number, details of the instruction to wash a car to the clothes in a machine or hand wash [8].

This might sound silly, but in an event that we have for long time been itching to have the capacity to check from any place on the planet, precisely what number of eggs is there in the fridge at our home, GE created an application based device known as the 'Egg Minder'. This device has a sensor just at the bottom of each cup where eggs are stored. The sensor transmits the information regarding the eggs, wirelessly to one's smart phone, feeding the details in the app installed in the phone (Figs. 2 and 3).

Architects nowadays use giant glasses covering the office buildings. These glasses tend to get heated up during the sunny afternoons, thus affecting the air conditioning inside the building. To cope up with this, "smart glasses" which combine the concept of Photo chromic and electro chromic technologies to build up a glass which transforms from clear glass to hazy or shady or tinted in seconds depending on the exposure of the sun-rays outside. These are examples based on

Fig. 2 Egg minder [9]

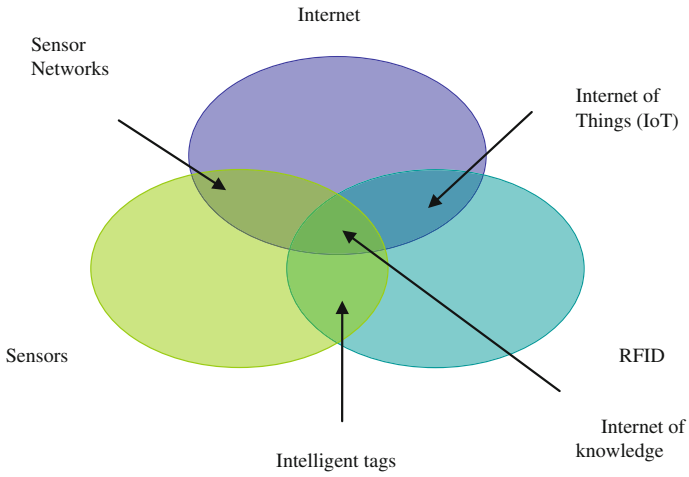

Fig. 3 Internet of things [10]

the concept of Internet of Things, by which we can say that in near future every object will have some knowledge and may have some level of mindfulness and self awareness [11, 9]. Soon there will be more objects connected in a network than humans. Every gadget we use daily would be have sensor soon and would work like a computer that has a microchip of its own.

Social networking is a network of people or organization which when put together as a set of actors forming a social structure among them. There would be a 'dyadic ties' i.e. interaction between these actors for the purpose of communication focusing mostly on social entity relationships [12] (Fig. 4).

The Internet of Things guarantees to be a wellspring of awesome advantages to our lives however it doubtlessly will be a wellspring of trouble for creators of

Fig. 4 Social internet of things [4]

telecom systems and applications unless suitable new correspondence ideal models are recognized. It can cooperate only among the objects which are of the same group. We absolutely accept that what will certainly address the issues of clients, planners, and engineers in a social way to deal with the Internet of Things. The targets being sought after by the Social Internet of Things (SIoT) ideal model are clear:

- To keep separate the two levels of individuals and things; to permit articles to have their own particular informal organizations.
- To permit people to force guidelines to ensure their protection and just get to the consequence of self-governing between article associations happening on the objects' interpersonal organization.

SIoT is a ''new time of miracle for science''. Social Communication sites, for example, Twitter, Instagram, Face book, LinkedIn etc., have pulled in the consideration of a huge number of researchers from a few regions [13]. As of late the thought that the merging of the ''Internet of Things'' and the ''Social Networks'' universes is conceivable, is picking up energy. This is because of the developing mindfulness that a ''Social Internet of Things'' (SIoT) ideal model would convey numerous attractive repercussions, soaking the normal existence of people. Additionally, plans have been suggested that utilization social connections to build larger amounts of trust, enhancing the productivity and adequacy of security arrangements [13]. Thus by Social Internet of Things we can say that every object is socially related creating a network which has smart objects connected socially.

Since the effect of the Internet age, more than 1 billion individuals have possessed the capacity to be joined with the World Wide Web, making obviously

unimaginable open doors for correspondence and joint effort. Due to today's fast moving life yet be connected to the world, electronic media and social networking play a vital role, people have started utilizing the Internet more than expected. This is all around the result of an overall population wide standard change in the uses and conceivable aftereffects of the Internet itself. The concept of social networking has been around since very long, people have always been social animals, working as groups, interacting with each other to get tasks done, helping others etc. This concept has been used over the internet and now it is bringing a major change in the definition of Internet which is now an important mode of connecting people. Social networking sites, like Face book, Twitter, Instagram, LinkedIn etc., in today's world is used to share thoughts, pictures, videos, information among themselves. This thought and idea is further utilized as a part of the late pattern and redesigning the concept of 'Internet of Things' to be called as 'Social Internet of Things'. Let us see an example, in the novels we generally find at the back cover, the information about the contents of the book. What if someday we cross a bookstore and pick up a book, turn to the back cover, scan the barcode using our smart phone and get directed to the YouTube video where author himself explains about the contents of the book. This social connection of human to things is a concept now being referred as SIoT [14].

The Internet of Things (IoT) connects a mixed bag of things around us that have the capacity to associate with every other and collaborate with their neighbours to interact with each other to complete a given task. The recently converged, 'Social Internet of Things' is an IoT where things are equipped for securing social associations with different articles, self-sufficiently as for people. Benefits of SIoT are as follows:

- Due to the SIoT structure, it can guarantee the framework navigability, so that the disclosure of things and organizations is performed reasonably
- Flexibility and scalability is guaranteed just like the humans, a level of dependability can be made for utilizing the level of collaboration among things that are companions or 'friends'. SIoT is based on the idea of friendship i.e. objects can search the required service by contacting the friends and friends of friends.
- The structures which have been designed for social networking can be used to address the challenges and issues which are related to IoT.

The main characteristics of SIoT are (Fig. 5)

- Scalability
- Fuzziness
- Heterogeneity
- Interoperability

The Architecture:
See (Figs. 6 and 7).

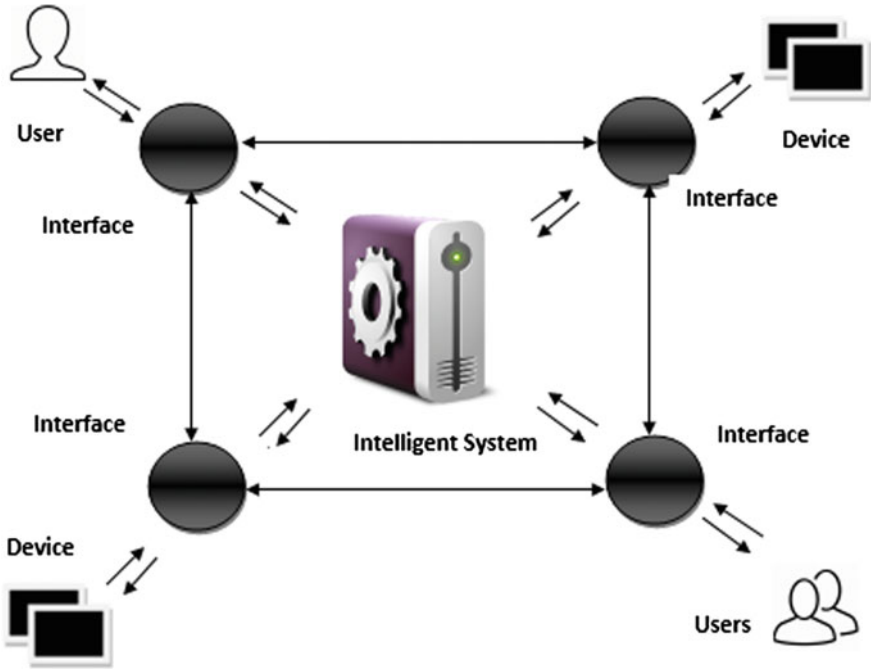

Fig. 5 General framework of SIoT

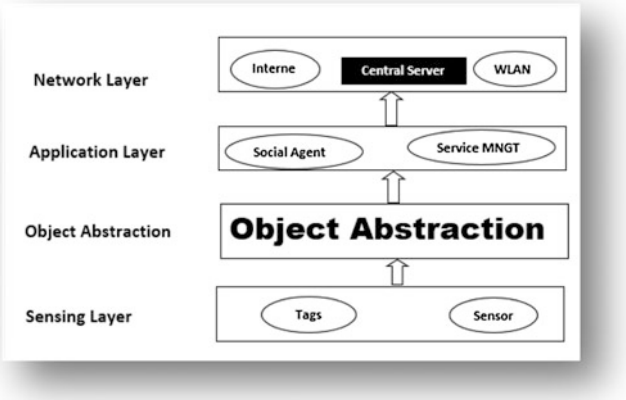

Fig. 6 Client side architecture

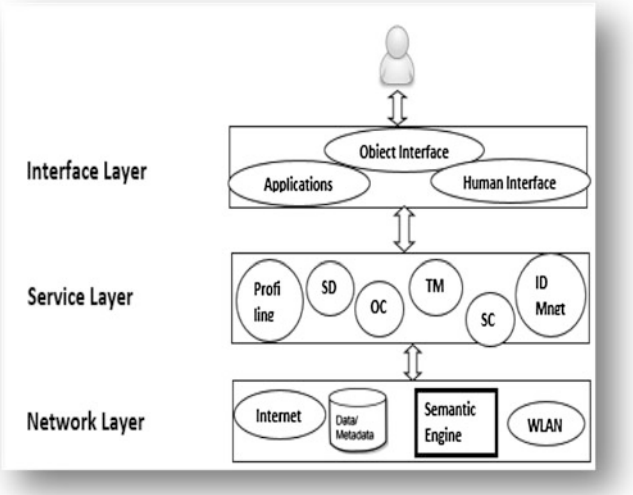

Fig. 7 Server side architecture

3 Advantages of SIoT

We present below some of the advantages of SIoT.

3.1 Navigability

A navigable network is one in which there exists a path to all or most existing nodes in the network [6]. Each node will have information of all the nodes in the setup and using distributed computation the nodes can exchange information. The idea is that all the nodes in the SIoT will have a short and direct path to each other. This improves the efficiency of sending and receiving data in the SIoT.

Currently the devices capable of being connected in IoT are increasing every day, hence the connection and access time for the things has increased. SIoT provides a way to reduce the access time of these devices through the use of social network. The nodes will be connected as friends and hence use that friendship to find the optimal navigable path [15]. Each node will have information of the surrounding nodes and utilizes that to select friends and navigate the global system. According to [6], a node will be allowed up to Nmax connections or friends and when it has the friends it can make use of the following heuristics to further make navigability possible:

- A node refuses any new request of friendships so that the connections are static.
- A node sorts its friends based on the degree they have so as to capitalize on the number of friends it will have from that connection.
- A node accepts new friendships and discards the old ones in order to minimize the number of nodes it can reach through its friends, i.e. to minimize the average degree of its friends; the node sorts its friends by their degree and the node with the highest value is discarded.
- A node accepts new friendships and discards the old ones in order to maximize its own local cluster coefficient; the node sorts its friends by the number of their common friends and the node with the lowest value is discarded.
- A node accepts new friendships and discards the old ones in order to minimize its own local cluster coefficient; the node sorts its friends by the number of their common friends and the node with the highest value is discarded.

The above mentioned heuristics are used by nodes to achieve navigability hence improving the search services and discovery of the nodes in SIoT. SIoT will provide a connection that is of low cost and independent of any private entity ownership. Systems will be deployed faster in this new system. [13] It provides a mechanism for things to communicate with each other, across regions, countries and through heterogeneous devices. It combines the physical world with the virtual technologically world into one seamless functioning system. The use of diverse technologies and small systems to make a huge intelligent system will change services and operations making them more efficient.

3.2 Flexibility

SIoT has adopted the social network behavior and structure which enable friends to discover each other and even connect through friends of friends. Nodes connected in SIoT will reduce the search time by adopting the friends' structure. Each node will have information about its friend or neighboring node and also its friend's friends. This eliminates the centralized traditional systems where every communication should generate from one designated point in a system and have a dedicated path to every other node. The SIoT becomes very flexible and has an added advantage over the existing systems.

It also has the ability of being resized as the need arises, it is by nature a distributed system hence adding or removing nodes will not affect the overall system performance. There is no limit as to the number of nodes that can be connected in a SIoT, it has a great advantage over normal centralized systems. In each connection nodes identify their friends and use those connections to scale the system as per need.

3.3 Trustworthiness

In SIoT each model will use its experiences and opinion of a friend to decide the service provider based on the level of trust shared. This increases the security of the SIoT because nodes will only communicate with their trusted friends. This will make isolation of malicious nodes possible and trustworthiness can be achieved through various models suggested by [16].

4 SIoT Challenges

Some challenges in SIoT are as follows:

4.1 Heterogeneous Devices

Several devices are connected in SIoT which include sensors, actuators, RFID tags or labels, mobile phones, computers and other embedded devices. In this text we will discuss more on the RFID because it's the major component of most or all SIOT applications and users.

The Radio Frequency Identification tags can be passive or battery assisted. As part of the system they pose the following challenges to SIOT:

- **(Uniform coding)** Many RFID tags are used in the SIoT and most of them will be from different vendors and having different formats. This is a huge challenge which at times affects the efficiency of the system. There is need to have a uniform encoding for all tags used and deployed in SIoT environment. Currently the two standards used for encoding are Universal Identification (UI) supported by Japan and Electronic Product Code (EPC) supported by Europe.
- **(Conflict collision)** Many RFIDs are deployed and are supposed to communicate together, this leads to the interference of signals and frequency, hence affecting the quality of data exchanged. Collision can occur in the form of tag collision which occurs there are a lot of labels to read from within a specific reader's radar causing it to fail reading the data correctly or reader collision occurs when the working scope of the reader overlaps and data becomes redundant weighing the network down.
- **(RFID privacy protection)** The RFID has no privacy protection and this makes the data vulnerable to malicious attacks during transmission. There is need for a lightweight privacy solution for the device to be protected. There are two aspects to consider in privacy protection that is data privacy and location privacy. Data privacy requires that there be a security solution for the data stored in the tag and location privacy involves protecting the exact location of the tag which can be accessed through the data stored in the tag.

- **(Trust management)** The RFID should have a mechanism that verifies whether a node is who it says it is. Trust management should start from the bottom of the SIoT and should be ensured in the tags that are used in the system [17, 18].

The devices in SIoT use different operating systems, protocols, languages and should communicate in real time. Interoperability can be achieved when there is a middleware in place, to enable communication across heterogeneous devices [19].

Each device must have the following in a SIoT environment:

- Identification in the network—there is needed to identify every node in the network using identification techniques available.
- A protocol for communication between devices.
- An open interface—devices should be able to communicate irrespective of the standards, operating systems and protocols used [19].

Given the above conditions SIoT faces the challenges of assigning addresses to the devices if they are in a dynamical setup, there has to be a mechanism to name the devices bearing in mind the fact that devices will not be static in the system. For example, when a smart phone wants to send data to other things and is currently in an area where there is no internet connectivity or other smart objects around.

Currently as to the best of our knowledge there is no universal communication protocol for things to use. This can affect the effectiveness of the SIoT if objects are not interoperable. Each device must be open to interact with the other devices. This can be achieved through the use of middleware, the main challenge would be which middleware should be adopted and will it be adopted by all things bearing in mind that each player in the SIoT will have its own brand and software. For example any device(thing) bearing the Microsoft brand will be inclined to use the DCOM middleware s compared to CORBA middleware and any java based thing will use Java Remote Method Invocation not Remote Procedure Call (SOAP or XML) [20].

4.2 Data Handling and Management

Communication in SIoT is viewed from two perspectives, data filtering and data storage. Each device will have its own format and also storage capacity which will differ. Most of the times any communication done in a SIoT will be in real time, for example sending traffic details to a smart car during traffic peak hours, monitoring the body reading of a patient, green house temperature readings etc. all these devices will be sending data per continuously, depending on the signal propagation method used there is bound to be various irrelevant data (noise) in the network. For the system to be efficient each component must have a mechanism in place that filters the data based on relevancy. After filtering the data should be in compatible format for all the devices to understand especially the receiver of that data. This process at times is required to be done in real time depending on the nature of the SIoT.

The data sent in the system needs to be stored and managed properly, the storage abilities of devices has increased vastly and this enables data to be stored at ease but separately through the use of distributed databases. However at some point even the conventional servers will not be able to store the data accumulated by these devices, there is need for big data storage and analytical skills to be adopted in SIoT for storing all the data [21]. Implementation of some of these aspects is a big hurdle in the success of SIoT and is still an open research challenge.

4.3 Energy Consumption Management

SIoT is composed of various devices which at times may be small and portable and battery powered. The major challenge with the energy consumption of the devices is they need to be charged up frequently and some batteries of devices deployed in the field may require changing after a few months or years depending upon the technology used. According to [21], all stages in the design of SIoT technologies have to be oriented to low-energy consumption.

Energy management affects the availability of the things which in turn affects the effectiveness of SIoT. The devices should be available at any time without fail for accurate performance. There is need to harness alternative energy methods for the devices deployed which last over years. [21]

One of the new technologies aimed at maintaining energy in the SIoT environments as mentioned by [7], is the Bluetooth 4.0, or BLE, which implements an entirely new protocol stack along with new profiles and applications. Its core objective is to run for a very long time on a coin-cell battery. It also enables devices to connect to the internet, where traditionally they have not been able to, in an efficient way through its client/server architecture. BLE is designed to be easy to develop for at a cheap price.

4.4 Security, Trust, and Privacy

Trust is a binary relationship between two entities, with one entity having confidence, belief and expectations that the other entity will act or intend to act beneficially. This is a trustor and trustee relationship, the trustor is the believing entity and the latter is the trustee [22, 23]. In SIoT trust has to be ensured amongst all the involved parties. Privacy refers to the user's anonymity and how safe they are in a particular location [24].

Security refers to techniques for ensuring that data stored in computing devices cannot be read or compromised by any individuals without authorization [23]. In SIoT devices information is transferred across the network with a high possibility of being accessed by unauthorized users. Security should enforce mechanism that

ensures that data will not be accessed by unauthorized users. The security aspect of the devices can be measured in the way a system ensures the following [25]:

- **Confidentiality:** Anything shared between entities should remain a secret and should not be accessed by unauthorised nodes; this aspect should protect the data from man in the middle attacks, and ensure the data is not understood by any intermediary. There are two aspects to consider in confidentiality according to [26], decision on storage and updating of security keys. In decision storage the nodes should decide on their own what data is to be stored locally and what is to be stored on servers or external locations. This gives the nodes more autonomy in decision making and helps them maintain confidentiality. Updating of security keys depends on the type of security used; there are two types of cryptography widely known namely symmetric key and asymmetric keys. The nodes should be able to decide which type to use based on factors like resource optimization and efficiency. The security keys should have solutions for untimely security breaches and a plan of what will be done when the security fails.
- **Integrity:** Data sent across the network has not been altered, to ensure integrity there is need to use digital signatures and hashing techniques when the nodes send their data. In the event that data has been altered, the nodes should be able to have a data log of when the data was altered during transmission and decide how to store these logs, locally or remotely. Integrity is also viewed in terms of the software running on the nodes; only authorized software should run on the nodes.
- **Privacy:** This refers to user anonymity and how safe they are in a particular location [24]. According to [26], the privacy policies should complement identification models for individual nodes and should give some amount of control to the user, if not all. The following goals are stated for privacy [26]:
  - Non-likability refers to the protection of the user's profile when they have several devices connected in a SIoT environment, there should be no connection to the user based on their devices.
  - Location privacy means the user's location should not be disclosed to anyone.
  - Content privacy means that no unauthorized user should have access to the content shared by a user in the system.
- **Availability:** The system should be available at all times to the users without interruption. The nodes should have access to all the components of the system. To ensure availability the system should be fault tolerant and scalable. Fault tolerance makes a system bounce back from attacks and scalability allows the system to grow in size without affecting performance of the system.
- **Access control:** The rightful user of the system has access to the data.
- **Non-repudiation**: Concrete proof that communication between entities occurred. Even when nodes are friends there is still the risk of denying communication after communicating.

- **Authorization:** The data is used by the authorized intended nodes.

To ensure security, trust and privacy the SIoT can utilize encryption algorithms, digital signatures and hashing techniques.

Therefore, summarizing the security aspect [25]:

Confidentiality refers to anything shared between entities should remain a secret. **Access control** refers to the rightful user of the system has access to the data.
Non-repudiation refers to concrete proof that communication between entities occurred. **Integrity** ensures that data sent across the network has not been altered.
Authorization means the data should be used by the authorized intended user. **Privacy** has the following aspects non-linkability, location privacy, content privacy and anonymity [26]. *Non-linkability* refers to the protection of the user's profile when they have several devices connected in a SIoT environment, there should be no connection to the user based on their devices. *Location privacy* means the user's location should not be disclosed to anyone. *Content privacy* means that no unauthorized user should have access to the content shared by a user in the system. **Availability** requires the system should be fault tolerant and scalable. To ensure security, trust and privacy the SIoT can utilize encryption algorithms, digital signatures and hashing techniques.

4.5 Resilience to Faults

According to Delic, system resilience refers to the capabilities to resist perturbances and crises, to recover from emergencies and near- catastrophes and the ability to adapt to a constantly changing environment [27]. Resilience to faults refers to the ability of the systems devices to bounce back after experiencing a technical fault. Any system is expected to have a mechanism for fault tolerance in the event that a fault occurs in one of the nodes. The devices in SIoT should be connected in a way that if one of them fails it can be removed or changed without affecting the whole system.

5 Some Recent Developments

Several developments have been made in putting SIoT in the proper perspective from different angles. In this section we present some of these taking their summaries.

5.1 Human Behavior

In [8] the potential of SIoT from the point of view of defining human behaviour was considered.

This work analyses the interactions and potential from the perspective of human dynamics, the potential of the Big Data and Smart Cities to increase our quantitative and qualitative understanding regarding the human behaviours.

The goal with the Internet of Things in the social area is to describe in real-time the human behaviours and activities. These goals are starting to be feasible through the quantity of data provided by the personal devices such as smart phone and the smart environments such as Smart cities that makes more intelligent the actions and the evolution of the ecosystem. Here, the ecosystem is analyzed defined by the triangle formed by Big Data, Smart cities and personal/Wearable computing to determine human behaviours and human dynamics.

A smart object, also known as an embedded device, thing or sensor is a physical element with the capability to be identifiable and optionally it can be also able to communicate sense and interact with the environment and other smart objects. They are considered smart since they can act intelligently under certain conditions through an autonomous behaviour.

Until now the IoT has been focused on supporting the interactions between machines, in order to send data to each other, carry out some actions under certain conditions and make feasible that heterogeneous objects interact among themselves.

Now the challenge is to define and understand the interactions between smart objects and humans. The origin of the Internet has been human-human type interactions, since the content was defined by humans to be consumed by other humans. Now with IoT the content being defined by objects, the interactions and influence over our lives is an open issue and this needs to be understood how the IoT will play a key role in our Smart Cities and Smart environments.

The IoT is defining an ecosystem, where it is not only a network to transfer data, else IoT also is interconnected with Big Data and Cloud computing to provide intelligence, in order to be able to understand the behaviours and even define actions according to the information captured by the smart objects that are able around the emerging smarter cities.

The potential of the Big Data and Smart cities for the human dynamics can be followed in three steps:

1. Define the new role of the citizens such as be prosumers
2. Understanding the human behaviours from the collected data
3. Influence into their behaviours through the continuous feedback.

Prosumer is a concept obtained by combining the words producer and consumer together. Prosumers are proactive consumers, who present a higher interest to stay connected, informed and participate, i.e. produce opinions, experiences, feelings and information. Since the creation of value is co-created with consumers, the value is no longer a single value creation from the enterprise, else that the prosumers

participate in the process of creating value through interaction with other customers and the enterprise.

Internet users create content online without interest. It can be found several courses, tips and video tutorials in the network of non-profit users. It can only also be found that the power of collaboration between multiple users for creating even greater resources. As an example Wikipedia provides the best example to date of the potential of collaborative intelligence and voluntary participation. Therefore, Big Data for prosumers and their behaviour peruses to analyses how is the activity from individual users to create a solution such as Wikipedia, in terms of participating, providing expertise for the company.

The understanding of behaviours is being carried out through the human dynamics for limited data source, such as logs from email servers and web browsers. The source and quantity of the data is changing drastically with the appearance of the social networks. But this continues increasing through the smart cities, where the data about the behaviour of the citizens and prosumers is also available from the real-life.

The challenge to encourage and motivate behaviour changes has been addressed by psychology for issues such as smoking cessation, increase exercise levels, drugs adherence and reduce energy consumption. Contextualized data can make the citizen; thereby influencing them to improve their behaviours.

5.2 Network Navigability

In [6] the concept of network navigability in the SIoT was considered along with its problems and some solutions. We summarize this attempt as follows.

A new paradigm known as Social Internet of Things has been introduced and proposes the integration of social networking concepts into the internet of things. The underneath idea is that every object can look for the desired service using its friendships, in a distributed manner.

However, in the resulting network, every object will still have to manage a large number of friends, slowing down the search of the services.

The intention is to address this issue by analyzing possible strategies to drive the objects to select the appropriate links for the benefit of overall network navigability.

A SIoT network is based on the idea that every object can look for the desired service by using its relationships, querying its friends, the friends of its friends and so on in a distributed manner, in order to guarantee an efficient and scalable discovery of objects and services following the same principles that characterize the social networks between humans. The assumption that a SIoT network will be navigable is based on the principle of the sociologist Stanley Milgram about the small-world phenomenon. This paradigm refers to the existence of short chains of acquaintances among individual in societies [28]. According to this paradigm, each object has to store and manage the information related to the friendships, implement the search functions, and eventually employ additional tools such as the trustworthiness relationship module to

evaluate the reliability of each friend [16]. Clearly, the number of relationships affects the memory consumption, the use of computational power and battery, and the efficacy of the service search operations. It results that the selection of the friendships is key for a successful deployment of the SIoT.

Five heuristics which are based on local network properties and that are expected to have an impact on the overall network structures. Then experiments were performed in terms of giant components, average degree of connections, local clustering and average path length.

The idea of using social networking elements in the IoT to allow objects to autonomously establish social relationships is gaining popularity in the last years. The driving motivation is that a social-oriented approach is expected to boost the discovery, selection and composition of services and information provided by distributed objects and networks that have access to the physical world [29–32]. Five different forms of socialization among objects are foreseen. These are,

1. Parental object relationship (POR)
2. Co-Location Object Relationship (CLOR)
3. Co-Work Object Relationship (CWOR)
4. Ownership Object relationship (OOR)
5. Social Object relationship (SOR)

5.3 Key Aspects of Network Navigability

In the past years, the problem of network navigability has been widely studied. As defined by Kleinberg [33], a network is navigable if it "contains short paths among all (or most) pairs of nodes". Several independent works, such as [34, 35], formally describe the condition for navigability: all, or the most of, the nodes must be connected, i.e. a giant component must exist in the network, and the effective diameter must be low.

When each node has full knowledge of the global network connectivity, finding short communication paths is merely a matter of distributed computation. However, this solution is not practical since there should be a centralized entity, which would have to handle the requests from all the objects, or the nodes themselves have to communicate and exchange information among each other; either way a huge amount of traffic would be generated.

In the SIoT, node similarity will depend on the particular service requested and on the types of relationships involved. The problem of global network navigability is then shifted to the problem of local network navigability, where neighboring nodes engage in negotiation to create, keep or discard their relations in order to create network hubs and clusters. The driving idea is to select a narrow set of links in order for a node to manage more efficiently its friendships. We first demonstrate how a SIoT network has the characteristics of navigability and then we apply

several heuristics for link selection and analyze the behavior of the network in terms of giant component, average degree, local cluster coefficient and average path length.

6 Scope for Future Work

As SIoT is a very recent topic and is yet to come out of its infancy, there is a lot of scope for research. However, we would like to point out a few of them in this Section.

8.6.1 Focus on the service discovery in network navigability and analyze the performance differences in finding the right object and service
8.6.2 Further analysis of application of small-world phenomenon in the context of SIoT
8.6.3 How to empower users in order to enable them to provide data with new gadgets such as glasses, watches and bracelets. These gadgets will extend the potential from the current smart phones
8.6.4 How to analyze the huge amounts of data in order to understand and discover the new models that describe the human dynamics
8.6.5 To define the proper and non-invasive mechanism, such as avatars, messages and metaphor mechanisms to offer feedback

The above are only a few from a pool of problems. Several such problems can be traced from the references provided below.

7 Conclusions

In this chapter, we started with the origin, history, development, challenges and current status of SIoT. Due to absence of knowledge and awareness we sometimes ignore ourselves and the environment in which we stay, by the way harming both. A few of the times this havoc is created and the environment is polluted knowingly being pretty aware of the after effects and also about the reasons behind such pollution and harm. Even it is hardly cared. It is said, that computers have the capability to persuade a human to bring about changes both in him and the other human beings. IoT and SIoT can take it as a challenge to influence people by providing awareness with surveys and data as a feedback from the others. Thus, can improve and influence human and their ignorance.

IoT with the help of social media can be a platform for changes and thus can make many unexpected or unimagined complex tasks simple with the help of connecting objects to objects intelligently and socially. This can create a new era of technology; a new revolution, if the right path is followed. Thus, smart cities can be built using smart and social environment. A data once produced can be guided to

form new applications connecting social objects by transforming and transferring data to form data over data. Therefore, with the help of IoT and SIoT, new challenges are being developed as to how to empower the human and their brains.

References

1. Postscrapes: Tracking the Internet of Things, a brief history of Internet of Things. http://postscapes.com/internet-of-things-history. Accessed 21 Jan 2015
2. Ashton, K.: That 'Internet of Things' Things, In the real world, things matter more than ideas, RFID J. http://www.rfidjournal.com/articles/view?4986 (2009). Accessed 29 Jan 2015
3. International Telecommunications Union: ITU Internet Reports 2005: The Internet of Things, Nov 2005. www.itu.int/internetofthings/ (2005). Accessed 21 Jan 2015
4. Social media on your wrist: Hicon is a bracelet that makes social networking wearable. http://iotevent.eu/application-2/social-media-wrist-hicon-bracelet-makes-social-networking-wearable-video/. Accessed 12 May 2015
5. darrel-j-butlin: Internet of Things made social. http://hexology.co/internet-of-things-made-social/ (2014). Accessed 7 Feb 2015
6. Nitti, M., Atzori, L., Cvijikj, I.P.: Friendship selection in the Social Internet of Things: challenges and possible strategies (2014)
7. Subramaniam, M., Ganesh, B.: Origin and applications of internet of things, cover story. CSI Commun. **38**(1) (2014). ISSN: 0970-647X
8. Jara, A.J., Bocchi, Y., Genoud, D.: Social Internet of things: the potential of the Internet of Things for defining human behaviour. In: International Conference on Intelligent Networking and Collaborative Systems, pp. 581–585 (2014)
9. Mims, C.: http://qz.com/100510/ge-just-invented-the-first-internet-of-things-device-youll-actually-want-to-own/ (2013)
10. Halfacree, G.: The Internet of Things gets some government cash. http://www.bit-tech.net/news/bits/2012/01/13/internet-of-things-government-cash/1 (2012). Accessed 30 Jan 2015
11. Mollman, S.: http://qz.com/409523/smart-glass-and-the-internet-of-things-will-make-your-office-less-stuffy/. Accessed 5 July 2015
12. http://en.wikipedia.org/wiki/Social_network. Accessed 5 July 2015
13. Atzori, L., Iera, A., Morabito, G., Nitti, M.: The social internet of things (SIoT)–when social networks meet the internet of things: concept, architecture and network characterization. Comput. Netw. **56**(16), 3594–3608 (2012)
14. Ruiz, S.G.: Social Things: When the Internet of Things Becomes Social. http://sugoru.com/2013/04/13/social-things-when-the-internet-of-things-becomes-social/ (2013). Accessed 4 July 2015
15. Chen, S., Xu, H., Liu, D., Hu, B., Wang, H.: A vision of IoT: applications, challenges, and opportunities with china perspective. IEEE Internet Things J. **1**(4), 349–359 (2014)
16. Nitti, M., Girau, R., Atzori, L.: Trustworthiness management in the social internet of things. IEEE Trans. Knowl. Data Eng. **26**(5), 1253–1266 (2014)
17. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of Things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
18. Xiu, D., Liu, Z.: A formal definition for trust in distributed systems. In: Information Security, pp. 482–489. Springer, Heidelberg (2005)
19. Efremov, S., Pilipenko, N., Voskov, L.: An integrated approach to common problems in the internet of things. Procedia Eng. **100**, 1215–1223 (2015)
20. Stephen, P., Kopack, M.: Teach Yourself Web Services in 24 Hours, 1st edn, pp. 64–66. SAMS publishing, Indianapolis, Indiana, USA (2003)

21. Ortiz, A.M., Hussein, D., Park, S., Han, S.N., Crespi, N.: The cluster between internet of things and social networks: review and research challenges. IEEE Internet Things J. **1**(3), 206–215 (2014)
22. Chen, Y.K.: Challenges and opportunities of internet of things. In: IEEE 17th Asia and South Pacific, Design Automation Conference (ASP-DAC), pp.383–388 (2012)
23. Beal, V.: Security Definition. http://www.webopedia.com/TERM/S/security.html. Accessed 4 June 2015
24. http://www.computerhope.com/jargon/p/privacy.html. Accessed 4 June 2015
25. Gunasekaran, A. (ed.).: Knowledge and Information Technology Management: Human and Social Perspectives. IGI Global (2002)
26. Ashraf, Q.M., Habaebi, M.H.: Autonomic schemes for threat mitigation in Internet of Things. J. Netw. Comput. Appl. **49**, 112–127 (2015)
27. Delic: Resilience to failure in: Resilience of IoT Systems. http://www.w3.org/2014/02/wot/papers/delic.pdf (2014). Accessed 4 June 2015
28. Travers, J., Milgram, S., Travers, J., Milgram, S.: An experimental study of the small world problem. Sociometry **32**, 425–443 (1969)
29. Mendes, P.: Social-driven internet of connected objects. In: Proceedings of the Interconnecting Smart Objects with the Internet Workshop, Mar 2011
30. Evangelos, A.K., Nikolaos, D.T., Anthony, C.B.: Integrating RFIDs and smart objects into a unified internet of things architecture. Adv. Internet Things (2011)
31. Atzori, L., Iera, A., Morabito, G.: SIoT: giving a social structure to the internet of things. IEEE Commun. Lett. **15**(11), 1193–1195 (2011)
32. Nitti, M., Girau, R., Atzori, L., Iera, A., Morabito, G.: A subjective model for trustworthiness evaluation in the social internet of things. In: 2012 IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), pp. 18–23. IEEE, Sept 2012
33. Boguna, M., Krioukov, D., Claffy, K.C.: Navigability of complex networks. Nat. Phys. **5**(1), 74–80 (2009)
34. Amaral, L.A., Ottino, J.M.: Complex networks. Eur. Phys. J. B-Condens. Matter Complex Syst. **38**(2), 147–162 (2004)
35. http://www.thinkgeek.com/product/162b/
36. Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., Qiu, D.: Security of the internet of things: Perspectives and challenges. Wirel Networks. **20**(8), 2481–2501 (2014)