A REVIEW ON TECHNOLOGY, ARCHITECTURE, APPLICATIONS, CHALLENGES AND FUTURE VISION OF INTERNET OF THINGS

V. R. Dunuwila
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology, Malabe, Sri Lanka
vandhana.d@sliit.lk

T. Tharsika
Department of Information Technology
Sri Lanka Institute of Information Technology,
Malabe, Sri Lanka
tharsika.t@sliit.lk

J. A. D. C. A. Jayakody
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology, Malabe, Sri Lanka
anuradha.j@sliit.lk

Abstract—**The Internet of Things (IoT) is a technology that enables objects to sense changes and respond involuntarily. It facilitates device to human communication, hence giving birth to the 'Smart' concept. The overall objective of conducting this review is to understand the present context of IoT. IoT utilizes technologies such as Radio Frequency Identification (RFID), Near Field Communication (NFC), Wireless Sensor Networks (WSNs) and Actuators to identify and track objects while technologies such as ZigBee, 3G, 4G, Bluetooth, and Wi-Fi facilitates communication among devices. The architecture model proposed for IoT is a multi-layered Service Oriented Architecture (SOA) consisting of six layers. IoT applications are already being deployed in various industries such as healthcare, manufacturing, logistics, supply chain and agriculture. The future of IoT inclines towards the introduction of Social Internet of Things (SIoT) and Sensing as a service, which initiated with the advent of cloud computing in IoT. Despite all the positives of IoT, the users also face certain technical, security, privacy, and legal challenges when working with IoT devices.**

Keywords-Internet of Things, Sensing as a Service, Smart concept, Service Oriented Architecture, RFID

I. INTRODUCTION

Internet of Things (IoT) has been an emerging technology in the past few decades, in which the Internet extends into the real world embracing everyday objects to bridge the gap between the virtual and the physical worlds [1,2]. Physical objects are no longer isolated but remain interactive as they can be controlled remotely. IoT has given rise to the 'Smart' concept in which smart devices, smart homes, smart cars and smart cities have become possible [2,3]. IoT utilizes sensors, actuators and communication technologies to cooperate and communicate with the physical objects as well as to interact with the people [1,2]. The capability of responding to events automatically and in real time opens up new opportunities for dealing with complex and critical situations, hence delivering substantial economic and social benefits [2,4]. Furthermore, these ITbased digital services can be accessed at not only a local level but also globally [5]. IoT, a concept that affects everyone and everything is a continually evolving research topic where opportunities are infinite [4].

The concept of IoT dates back to 1982 when a coke machine at Carnegie Mellon University, Pennsylvania was connected to the internet to check the status of the machine and determine whether the drinks were cold or not [4, 6]. In 1991 Mark Weiser visualized Internet of Things in the form of ubiquitous computing. Later in 1999, a clue on device-to device communication was same year, the word 'Internet of Things' was proposed by Kevin Ashton, the Executive Director of Auto-ID Labs in Massachusetts Institute of Technology (MIT) when describing a system of interconnected devices [2,4,6]. The concept of IoT was popularized by the work of the Auto-ID Centre at MIT when they designed and propagated a cross-company RFID infrastructure [2,6].

Later in the year, Neil Gershenfeld also spoke about IoT in his book titled "When Things Start to Think". In the year, 2000 LG launched their first Internet of refrigerator plans. RFID was deployed by the US Department of Defence in 2003 and in Wal-Mart by 2004 [6]. In 2005, the first report on IoT was published at the UN's International Telecommunications Union (ITU). IoT was also listed as one of the six "Disruptive Civil Technologies" by the US National Intelligence Council in 2008 [6]. Furthermore, the first scientific conference on IoT recognized by the EU Commission was held in the same year [6]. IoT has continued to evolve in the past few years and many more conferences and researches have been conducted over the years [2].

IoT technology is widely used in many areas such as manufacturing, logistics, supply chain management, healthcare, mining, firefighting, traffic controlling, agriculture, security and weather forecasting [1,4,7]. The key technologies of IoT include RFID's and Wireless Sensor Networks (WSNs). RFID identifies, tracks, and monitors objects attached with RFID tags while WSNs sense and monitor characteristics of the environment and its objects. Both RFID's and WSNs have contributed significantly to the development of IoT [1]. These devices embedded with IoT technology have the capability to sense and respond to situations automatically [6, 8].

Currently most organizations such as the International Telecommunication Union, International Organization for Standardization, IEEE, European Committee for Electrotechnical Standardization and American National

Standards Institute are interested in developing standards for IoT so that effective information exchange, processing, and communication can be ensured, while saving the development and maintenance cost in the long run and promoting continuous innovation of IoT [1,6,8].

II.RESEARCH OBJECTIVES

This paper reviews the literature surrounding Internet of Things (IoT), its key technologies, architecture, applications, challenges and areas of future research.

The overall objective of this literature review is to understand the present context of IoT. Our specific objectives include: to determine the key technologies associated with Internet of Things, to explore the different architecture models proposed for IoT, to gain an understanding of the IoT applications deployed in various industries, to Fig. out the key challenges of using IoT, to determine the future vision of IoT and to identify the areas of future research.

Section III of this paper discusses the key technologies that facilitate IoT while Section IV talks about the different architecture models proposed for IoT. Section V describes different applications of IoT that are already being used in the industry. The next section, Section VI illustrates the different challenges that users have to go through in utilizing IoT while Section VII points out the future vision of IoT. Finally, Section VIII discusses the areas of future research in IoT.

III.KEY TECHNOLOGIES OF IOT

The Internet of Things is not a solitary novel innovation but a combination of several technologies that minimizes the inconsistency between the virtual and physical worlds. These technologies enable objects to sense, identify, actuate, communicate, cooperate, and localize¬ [2].

A. Identification and tracking technologies

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

The most common identification and tracking technologies involved with IoT include RFID systems and intelligent sensors [1].

1) Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) is a technology that transmits the identity of an object or person wirelessly using radio waves in the form of a serial number [6]. The RFID system comprises of RFID readers and RFID tags. These tags could be either active or passive [4, 6]. Active tags are more costly and remain dynamic all the time as they have a battery attached to them while passive tags are activated only when a signal is generated [4]. The tags contain different forms of data, but the most commonly used form of data in IoT applications is the Electronic Product Code, or EPC.

An EPC is a universally unique identifier for an object, which ensures that each object would have distinctiveness in

IoT [9]. The RFID tags emit identification, location or any other information about the object, which is transmitted to the RFID readers using radio frequencies that are then passed onto the processors for data analysis [4]. Due to its capability of identifying and tracking objects in real time, the RFID system is increasingly being utilized in logistics, supply chain management, aviation, and healthcare service monitoring [1,4,9]. The benefits of using RFID include the availability of precise real-time information about the devices, which simplifies business processes hence reducing labor costs and improving business efficiency [1,4].

2) Barcodes

Barcode is also an identification technology that performs the same role as RFID [4]. It identifies objects by reading the optical label that records information about the object. Barcodes are usually read by laser scanners and can be also

read using a camera [6]. Since barcodes utilize optical technology, the object needs to be placed in front of the reader for identification while RFID does not require the object to be physically present in the vicinity. Furthermore, RFID can act as an actuator that can trigger and modify events whereas barcodes cannot [4].

3) Near Field Communication (NFC)

Near Field Communication (NFC) is a short-range wireless technology that enables devices to communicate through radio frequencies when brought close to each other. It is a novel technology that is built in accordance with the RFID framework [9]. NFC helps makes consumers lives convenient by being able to connect electronic devices and exchange information with a touch of a button [6]. NFC tags contain a Unique Identification (UID) that helps objects to be uniquely identified. This technology is most commonly used with smart phones where information exchange is possible once the devices are brought together [9].

4) Wireless Sensor Networks (WSNs)

Sensors monitor and collect data regarding the characteristics of the environment and objects such as temperature, sound, vibration, pressure, humidity, movement, and quantity [4,6,9]. A wireless sensor network is a network of multiple wireless sensors that are autonomously distributed yet interactive [4,6,9]. In the network, one node will be connected to one or more nodes [4]. WSN's are bi-directional and follow multi hop fashion when communicating among the sensing nodes [4]. WSN's contain sensors and gateways within themselves to collect and transmit data to a server rapidly [9]. WSN's are used

in many broad areas such as military, household security, healthcare, agriculture monitoring, manufacturing, habitat monitoring and natural disaster detection [6]. When combined with RFID, Wireless Sensor Networks create potential for even smarter devices with better tracking and tracing functionalities in real time [1,4]. Intelligent sensors have been developed using infrared, γ-ray, pressure, vibration, electromagnetic, and X-ray to assist analysis and decision making [8].

5) Actuators

While sensors monitor the physical conditions of the environment and objects, actuators have the ability to sense and respond to external stimuli [9]. They convert energy to motion in order to affect the environment or the object [6]. Actuators are capable of emitting sound, light, radio waves or even odours. Actuators are used together with sensors to form a sensor-actuator network. These networks have the ability to sense and respond to vulnerable situations [9]. For instance the existence of Carbon monoxide in a room will be sensed by the network and immediate action will be taken by producing a loud noise to alert people about it. The integration of sensors and actuators enable objects to communicate and interact with people effectively [9]. Actuators are most commonly used in manufacturing and industrial applications [6].

B. Networking and Communication technologies

All devices in an IoT network must be organized in a way that they are accessible for communication. However, the communication requirements and technologies may vary from one device to another [8]. A fast and effective network is required to facilitate communication among a large number of devices [4].

IoT is an integration of several heterogeneous networks such as WSNs, wireless mesh networks, mobile networks and WLAN's [1,8]. Mobile networks have become unpredictable due to the evolution of a super-fast and superefficient fifth generation wireless systems that offer more bandwidth [4].

Gateways are capable of enhancing interaction and communication among IoT devices, hence are used in complex decision-making [1,8]. The use of IPv6 has benefited people as addressing things directly through the internet is now possible [1].

3G and 4G are used for wide range transmissions whereas Bluetooth and Wi-Fi are used for short-range communication [4]. Wi-Fi allows computers and other devices to communicate over a wireless media whereas Bluetooth facilitates information sharing, eliminating the need for cabling the two devices. ZigBee is a protocol that enhances the functionalities of Wireless Sensor Networks which makes them scalable, reliable and flexible [6].

The most common communication protocols and standards include RFID, NFC, WLAN, ZigBee, Bluetooth, Multihop Wireless Sensor/Mesh Networks, IETF Low Power Wireless Personal Area Networks (6LoWPAN), Machine-to-Machine (M2M), and traditional IP technologies such as IP, IPv6 [1,8]

IV.IOT ARCHITECTURE

The number of IoT devices are increasing at a rapid rate and is expected to have more than 25 Billion devices connected by 2020 [4]. It is important that these devices stay connected in order to bridge the gap between the physical and virtual worlds [8]. The existing internet architecture that uses the TCP/IP protocol is incapable of handling a large network connected to billions of things [4]. This required a new architecture for IoT that would be scalable, adaptive and interoperable with heterogeneous devices while addressing the security and Quality of Service issues [4,8]. Hence, a service-oriented architecture (SOA) was introduced for IoT that ensures interoperability among heterogeneous devices in multiple ways [1,8].

Several multi-layered architectures were proposed for IoT [4,10] described a three-layer architecture which consisted of perception, network and application layers while [1,8] described a four key level architecture that comprised of sensing, networking, service and interface layers [6]. described a five-layer architecture consisting of sensing, access, network, middleware and application layers. Similarly, a six-layered architecture was proposed in [4] that had better functionalities and consisted of a coding, perception, network, middleware, application and business layers.

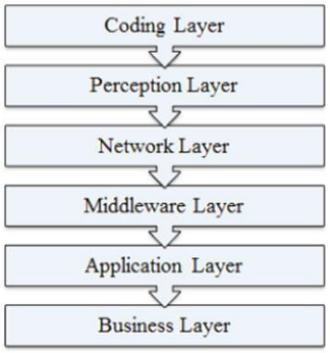

Fig. 1. Six Layered Architecture proposed for IoT [4]

A. Coding Layer

The coding layer is the base of IoT that assigns a unique ID for each object hence they could be easily identified [4,8]. This technique is called universal unique identifier (UUID) where every object would hold a digital identity to ease tracking and retrieval [1,8]. UUID's are critical for the success of IoT networks [1,8].

B. Perception Layer

The perception layer described in [4,10] performs the same functionality as the sensing layer in [1,8]. This layer contains the physical devices that sense and exchange information using RFID tags, IR sensors and sensor

networks [1,4,10]. The information collected here will be converted to digital signals so that it can be passed on to the network layer [4].

C. Network Layer

The network layer is the infrastructure that connects everything together while facilitating the sharing of information among IoT devices [1,8]. It receives digital signals from the perception layer that is then transmitted to the middleware layer through mediums such as Wifi, Bluetooth, WiMaX, ZigBee, CDMA, GSM and 3G [4,10]. The network layer also aggregates data from existing IT infrastructures before transmitting them to the middleware layer [8, 1].

D. Middleware Layer

The middleware layer described in [4,6] performs the same function as the service layer described in [1,8]. It uses platform independent middleware such as Open Sensor Web Architecture (OSWA) to bridge network infrastructure and IoT architecture that uses different protocols, standards so that information received from the network layer can be processed, and the relevant action can be taken [1,4,8,11].

E. Application Layer

The application layer described in [4,6,10] is very much similar to the interface layer described in [1,8]. Here the users interact with IoT applications such as smart homes, smart environments and smart businesses [4,10]. The application layer contributes in promoting the development of the IoT network by introducing new applications regularly [4]. It uses an interface profile (IFP) to facilitate the interaction with applications deployed in the network [1,8].

F. Business Layer

The business layer deals with the administration of IoT and is responsible for further exploration of IoT. It produces diverse plans of action for successful business strategies [4].

However, despite the multilayered service-oriented architecture models described in [1,4,6,8,10,12] illustrates a Semantic Fusion model which uses a smart semantic framework to capture data from sensor networks. According to [12], the Semantic Fusion model has three visions. They are the Things oriented vision, Internet oriented vision and the semantic oriented vision.

The Things oriented vision states that it is possible to track anything using sensors and technologies such as RFID. It believes in using Electronic Product Code (EPC) to identify objects uniquely. The Internet oriented vision focuses on objects that are connected in which the data in the objects are converted to a meaningful format so that it can be uniquely identified [12]. The semantic oriented vision ensures that the raw data from the vast amount of sensors are managed and processed for better understanding [12].

V.IOT SERVICES AND APPLICATIONS

Although most of the applications that we utilize daily are smart, they are incapable of communicating and sharing information with each other [4]. In the meantime, IoT applications emerged which contributed significantly to improve the quality of living by making life easier, safe and smart [4,7]. Currently IoT applications are deployed in several industries including healthcare, manufacturing and traffic controlling [1,8]. These applications are still in an early stage but are seen to evolve rapidly [1].

A. Smart health

IoT has been able to improve the quality of human life by automating tasks such as monitoring and decision making that was performed by humans previously [9]. Patients would be provided a wearable device embedded with RFID so that the doctors and nurses are able to monitor the heart rate, temperature and blood pressure even when they are not within the hospital premises [4]. Hence, IoT technologies take better care of the patients whilst reducing the cost of traditional care [7]. Furthermore, RFID chips can be implanted in the patient's body to detect abnormalities and thus alert the doctor in the case of an emergency [12]. In the case of cardiac emergencies, drone ambulances with an emergency kit would be able to reach the patient faster than usual ambulances [4]. The threat of new medications in terms of allergies can also be evaluated using IoT sensors
[1].

B. Smart homes

IoT automates many of our household needs by providing Do-It-Yourself solutions while controlling appliances as per our requirement [4]. It takes control over electronic appliances such as air conditioners, refrigerators and washing machines hence saving energy [11]. We would be able to monitor our utility meters and detect leaks well in advance. IoT sensors could be used to prevent burglaries and they are also useful in measuring temperature, humidity and moisture in the environment. Furthermore, it facilitates gardening by watering plants according to their requirement [4].

C. Smart traffic systems

Traffic congestion has become a dominant problem in the society, which is difficult to resolve [4]. Every single traffic congestion accounts to the loss of fuel resulting a huge loss in terms of economy. With the intention of finding a solution to this problem, Traffic IoT (TIoT) was introduced [12]. Traffic IoT uses sensor-enabled communication to provide a good transportation experience by reporting traffic congestions and accidents to drivers so that they could use alternative roads [4,12]. It would report the current state of traffic conditions to avoid unexpected traffic jams [12]. In addition, it would show the availability of parking spaces on roads and facilitate theft detection of vehicles [4]. Automobiles have been provided with autopilot functionalities that detect pedestrians and other vehicles and act accordingly to avoid collisions [1].

D. IoT in Logistics and Supply chain management

RFID and sensor networks play a major role in supply chain management. Sensors are used in assembly lines while RFID is frequently used to track products in any part of the supply chain from manufacturing to distribution [1, 9]. The pervasiveness and ubiquity of IoT has enabled detailed and

up-to date information exchange across geographical boundaries hence improving supply chain efficiency [9]. RFID also assists retailers in tracking the stock to prevent zero inventory situations by placing an order automatically [4]. IoT also plays an important role in logistics by conducting real time monitoring of physical objects moving from one destination to another across the entire supply chain. An intelligent informatics system known as iDrive was introduced by BMW to track the location of the vehicle and provide directions to the driver [1].

E. Smart grids

Smart grids have been developed to ensure a smart energy management. It is able to integrate information and communications technologies to electricity so that two-way communication will be created between suppliers and consumers, which results in delivering electricity more efficiently and sustainably [7]. The energy consumption of any given locality can be efficiently monitored using smart meters [7,12]. Furthermore, smart grids promote a green environment by reducing the level of carbon emissions whilst benefitting the customer by saving cost through the efficient use of energy [7].

F. Smart agriculture

IoT is used in agriculture for various purposes. It uses sensor networks to monitor the production of vegetables and fruits under fluctuating environmental conditions such as weather, water, and sunlight [7]. In addition, these sensors monitor the nutrition in the soil to increase the production of grains and prevent loss of crops [4,12]. Watering will be done as per the requirement of each plant, which limits the wastage of water [13].

G. Smart environment

The environment plays a major role in our lives. Not only humans but birds, plants, fishes and animals are all affected by the environment. IoT is used in a smart environment for various purposes [7]. It is used to measure the levels of air and water pollution while controlling waste management by monitoring industrial pollution in real time [7]. IoT also provides accurate weather information and predicts natural disasters well in advance so that its impact can be minimized to a greater extent [4,7].

H. Social IoT (SIoT)

SIoT portrays how things and human beings can be intelligently sensed and networked similar to human social networks [8]. IoT devices promote social interactions by integrating with social media platforms such as Facebook and twitter to provide information on an individual's whereabouts. These applications collect data and inform the relevant individuals based on activities that may interest them [9].This required a new architecture for IoT that would be scalable, adaptive and interoperable with heterogeneous devices while addressing the security and Quality of Service issues [4,8]. Hence, a service-oriented architecture (SOA) was introduced for IoT that ensures interoperability among heterogeneous devices in multiple ways [1,8].

VI.CHALLENGES IN IOT

Despite the presence of appealing applications, IoT has its challenges as well [2,4,7,9]. Progressing from the internet of computers to the internet of things is not an easy task. For IoT to succeed, it must be available at a low cost that users can afford [2,7]. In addition, there are some other challenges that haves to be overcome to ensure the successful implementation of IoT [2,7,9]. According to [4,7] the most common technical challenges include:

- Configuring smart devices
- Interoperability between devices Scalability of the IoT network
- The cComplexity of the software used
- Powering devices that move around
- Dealing with large data volumes
- Ensuring a fault tolerant IoT network
- Interpreting sensed raw data

Furthermore [2,4,7,9] describes security and privacy challenges that needs to be resolved.

- Confidentiality, Authenticity & Integrity of communication
- Inability to support robust encryption of IoT devices
- The threat to personal privacy and issues with data ownership
- Unauthorized access to RFID - RFID Virus, Side Channel Attack, SpeedPass Hack
- Sensor nodes security breach - Jamming, Tampering, Sybil attack, Flooding
- Cloud computing abuse – Man in the middle attack,
- Phishing, Malicious Insider, Data loss, Account Hijacking

According to [9] IoT will create new legal challenges that must be mitigated by establishing a governance structure where the responsibility is shared, and the users are held accountable.,

VII.FUTURE OF IOT

Since IoT is a novel concept, it would continue to evolve in the future. Its scope would expand, and new technologies would emerge.

[9] predicts two of such future visions for IoT. Researchers believe that IoT would mash up with Web 2.0 to create a Web of Things that would use web standards to fully integrate smart objects into the World Wide Web. They also believe that more and more nano scale devices with communication networks would be interconnected to form an Internet of Nano-Things [9].

According to [14] the future of IoT inclines towards Social Internet of Things (SIoT). While IoT focuses on devices that sense and actuate physical objects, SIoT is concerned withon why and how users utilize these services and applications in their everyday life. The increasing sociality and pervasiveness of the internet improves the relationship between humans and things [9]. Social networks provide proactive and reactive information such as interests,

locations, demographics and characteristics of relationships. Social network users tend to utilize these social aspects in their decision-making [9]. Hence humans and things are no longer isolated and their objectives and needs entwine together to form the SIoT. This improves the availability of both humans and things while assuring transparency as well

[9].

[7] states that the trend of IoT is towards cloud computing distributed computing and fog computing. Cloud computing has the capability to facilitate service management and the implementation of IoT applications as well as deal with real world objects in a more dynamic manner. The cloud acts as an intermediary layer between the objects and the applications by eliminating all complexities [7]. Further, the cloud environment would facilitate IoT applications in data collection, data processing while maintaining low costs for deployment and creating new opportunities for data aggregation, integration and sharing of data with third parties [7].

The use of distributed computing in IoT would enable physical objects to be remotely controlled while they act as physical access points to the internet [7]. Fog platforms have dense computational architectures, which include characteristics such as location awareness, wireless access and focuses on performing analytics. IoT is more likely to be facilitated by fog computing in the future [7].

According to [13,15] in future, IoT would be applied in an urban context to develop Smart cities. The objectives of developing smart cities would be to ensure a better use of public infrastructure and to increase the quality of services offered to citizens while reducing the operational costs of the government [15]. Benefits of adopting smart cities would include optimization of public services, such as transport, surveillance, maintenance and waste management [15].

Smart cities would use sensing as a service model to perform functionalities such as: Air quality monitoring, noise monitoring, traffic congestion controlling, smart parking, smart lighting and smart city energy consumption where most of these would be powered by batteries and photovoltaic cells [13,15].

In future, IoT would facilitate waste management of smart cities to a great extent [13,15]. They would use sensed data to develop optimized garbage collection strategies, in which they can save the fuel cost of garbage trucks [13]. Furthermore, recycling companies can use data from sensors to predict and track the amount of waste coming into their plants to be processed so that their internal processes can be optimized to suit the requirement. Apart from that, authorities can monitor and supervise the waste management process at a low cost by saving money spent on manual inspections [13].

VIII. FUTURE RESEARCH

The analysis of IoT related literature revealed several open challenges for research. Since IoT is still an area under discussion, the majority of the contemporary papers focused on its technology and most of the researches were conducted by Asian and European countries. Hence, IoT literature is dominated by research relating to IoT technology performed by Asian and European researchers.

Very less research has been carried out regarding the use of IoT driven business models and the use of IoT in areas such as law, economics and sociology are to be investigated [9]. This gives rise to several questions described in [9] that need to be answered in future research. The questions include:

- What kind of theories and models of IoT could be used for the management and operations of businesses and commerce?
- How can information systems working with IoT fit in with the Big data concept to overcome the complexity and data volume to facilitate decision making?
- What are the unaddressed application areas of IoT?

IoT innovators are currently facing problems related to device level energy supply, identification and addressing of devices, scalability of the Internet as well as the security and personal privacy of the users [5].

As IoT utilizes countless amounts of sensors, their power consumption has become a big concern [1]. Most of these sensors are powered by battery or photovoltaic cells [13]. Researchers should focus on developing green IoT technologies that would be energy efficient thereby saving energy through the reduction of the power consumed by sensors [1].

Since a single IoT device can sense a number of parameters, the same data can be used to derive many conclusions. Hence, IoT could be paired with cloud computing to facilitate better connectivity between objects [1]. Research has to be carried out to focus on implementing new models that would provide “sensing as a service” on the cloud [1,13].

Developing middleware that can facilitate billions of sensors is one of the major challenges faced by sensing as a service model. In order to cater to the high demand, sensing as a service requires upgrading its data communication bandwidth over the existing infrastructure [13]. Furthermore, researchers should explore the standardization of sensing as a service technology as it is the key to interoperability [13]. Since sensing, as a service model is a novel concept, trust and acceptance is vital for its success. Hence new security protocols need to be established to win the trust of all parties involved [13].

Although several architecture models have been proposed for IoT, designing a service-oriented architecture (SoA) model has been challenging. An effort has to be placed in determining a service-based architecture for IoT, with its performance, service composition and cost components [8]. Furthermore, there is a need for a common accepted service language that would be compatible in

different implementation environments together with a powerful search engine to locate objects in an IoT network [8].

The services of the majority of the IoT devices end with notifying the customer about what it sensed which requires users to take actions manually. Therefore, future researchers should focus on developing standards and protocols to enable machine-to-machine (M2M) communication [4,13].

The success of an organization offering IoT products would depend on the IoT platform that the company would be using [5]. Hence, researchers should focus on investigating the capabilities of platform providers to build active ecosystems and provide professional and timely support for organizations [5].

Since IoT uses billions of sensors, it is impossible to process all the data collected through these sensors [1]. Middleware has been proposed to overcome this problem but most of the IoT middleware solutions do not have context awareness capabilities. Therefore, this is considered to be one of the most important future research areas in IoT [1].

Most of the IoT applications involve human interaction where humans and objects operate synergistically giving rise to human-in-the-loop systems [3]. There is a need for a broad understanding of human-in-the-loop systems and its controls as well as to derive human behaviour models and determine how these behaviour models could be used in providing feedback [3]. Human-in-the-loop systems have become an emerging trend in IoT that needs to be further explored.

IX.CONCLUSION

The purpose of this review was to understand the present context of IoT. The Internet of Things is a network of objects that are capable of communicating with each other using standard and interoperable communication protocols in order to bridge the gap between the virtual and physical worlds. IoT devices are capable of sensing changes and responding to them in real time. The concept of IoT has given rise to several applications related to smart health, smart homes, smart cities and smart environments. IoT also assists manufacturing organizations by facilitating logistics and supply chain management.

Technologies such as RFID and WSNs are frequently used in identifying and tracking objects whereas technologies such as Bluetooth, Wi-Fi and ZigBee facilitate communication among a large number of devices. The incapability of the TCP/IP protocol to handle a large network of heterogeneous devices, led to the introduction of a multi layered service-oriented architecture model that ensured interoperability among different devices. However, there are few privacy and security challenges that are to be overcome in addition to the prevalent legal and technical issues.

Social Internet of Things (SIoT), Internet of Nano-Things and smart cities have become the future vision of IoT whereas sensing as a service has been introduced with the advent of cloud computing in IoT. Further research is required to develop green IoT technologies that are energy efficient and to develop standards and protocols to enable machine-to-machine (M2M) communication.

ACKNOWLEDGMENT

This work was supported by Sri Lanka Institute of Information Technology.

REFERENCES

[1] . D. Su, S. Li and W. He, "Internet of Things in Industries: A Survey," IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, vol. 10, no. 4, pp. 2233-2243, 2014.

[2] F. Mattern and C. Floerkemeier, "From the Internet of Computers to Internet of Things," From Active Data Management to Event-Based Systems and More, vol. 6462, pp. 242-259, 2015.

[3] J. A. Stankovic, "Research Directions for the Internet of Things," IEEE Internet of Things Journal , vol. 1, no. 1, pp. 3-9, 2014.

[4] M. U. Farooq, M. Waseem, S. Mazhar, A. Khairi and T. Kamal, "A Review on Internet of Things (IoT)," International Journal of Computer Applications, vol. 113, no. 1, 2015.

[5] F. Wortmann and K. Flüchter, "Internet of Things - Technology and Value Added," Business & Information Systems Engineering, vol. 57, no. 3, pp. 221-224, 2015.

[6] S. Madakam, R. Ramaswamy and S. Tripathi, "Internet of Things (Communications, IoT): A Literature vol. 3, pp. 164Review," -173, 2015. Journal of Computer and

[7] Z. K. A. Mohammed and E. S. A. Ahmed, "Internet of Things Applications, Challenges and Related Future Technologies," World Scientific News, vol. 67, no. 2, pp. 126-148, 2017.

[8] S. Li, L. D. Xu and S. Zhao, "The internet of things: a survey, Information Systems Frontiers, vol. 17, no. 2, p. 243–259, 2015.

[9] A. Whitmore, A. Agarwal and L. D. Xu, "The Internet of Things—A survey of topics and trends," Information System Frontiers, vol. 17, p. 261–274, 2015.

[10] A. Khalid, "Internet of Thing Architecture and Research Agenda," International Journal of Computer Science and Mobile Computing, vol. 5, no. 3, p. 351 – 356, 2016.

[11] G. Jayavardhana, B. Rajkumar, M. Slaven and P. Marimuthu, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645-1660, 2013.

[12] D. Singh, G. Tripathi and A. J. Jara, "A survey of Internet-of-Things: Future Vision, Architecture, Challenges and Services," in 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, 2014. [13] C. Perera, A. Zaslavsky, D. Georgakopoulos and P. Christen, "Sensing as a Service Model for Smart Cities Supported by Internet of Things," TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES, pp. 1-12, 2014.

[14] A. M. Ortiz, S. Park, S. N. Han, N. Crespi and D. Hussein, "The Cluster Between Internet of Things and Social Networks: Review and Research Challenges," IEEE Internet of Things Journal, vol. 1, no. 3, pp. 206-2015, 2014.

[15] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, "Internet of Things for Smart Cities," IEEE INTERNET OF THINGS JOURNAL, vol. 1, no. 1, pp. 22-33, 2014.

[16] J. Jin, G. Jayavardhana, S. Marusic and M. Palaniswami, "An Information FrameworkThings," IEEE Internet of Things Journal, for Creating a Smart City Through vol. 1, no. 2, pp. 112 Internet of - 121,2014