I J C T A, 9(15), 2016, pp. 7351-7359

An overview of the Internet of Things and its Research Issues

Ravindra[1], Chandra K. Jha[2], Ashish Kr. Luhach[*3] and Shiv Preet[4]

ABSTRACT

The growth in Information and communication technology (ICT) changed our lives and integrated a virtual world into our professional lives as well. IoT has the potential to give a new direction to this by enabling the communication between the physical objects and humans through internet. IoT is to be believed as the biggest revolution in technology and the growth rate of IoT is 270% in last six year, which is much higher than the growth rate of smart mobile phones. This research paper, studied about all the important aspects and atomic components related to IoT. In this research paper, we explored the requirement related to full development of IoT. Later, this research paper focused on research issues which are still open in IoT in terms of standardization, networking and security.

1. INTRODUCTION

In last decade, the computing world has experienced a revolution in technology which also has significant impact on our daily lives as well. The smart phones, tablets and laptops became an integral part of our professional and personal lives. The number of internet user increases significantly in this period. We have enlarged emerging space of interconnected devices. This era of information and communication technology (ICT) is not only focused on the nurturing of networks and communication between humans but also facilities the connection between humans and things, to form a network of human and things termed as Internet of Things (IoT). IoT to be believed as the biggest revolution in technology and the growth rate of IoT is 270% in last six year, which is much higher than the growth rate of smart mobile phones [1]. Many larger cooperate and even governments are funding for the research on IoT. In fact, IoT is going to play a significant role in shaping up the smart cities. A home user is also going to be influenced by applications of IoT such as smart thermostat, smart houses and smart cars etc. For corporate environment, IoT helps them in enabling the computerization of their work and also provide a smarter and reliable environment for their employee, which leads to the reduction of their expenses [2]. IoT is coming to achieve their above mentioned objectives by proper combination and utilization of the existing technologies with each other such as smart sensors and meters, and Radio Frequency Identifiers (RFIDs). These technologies are integrated into each other to formulate a new embryonic behavior of IoT.

Before the thought of IoT being broadly acknowledged, many issues need to be tended and both technical and social have to be unchained. One of the major issues is to make fully interoperable system consist of various interconnected devices and provide them a higher degree of smartness while guaranteeing the security for the same. This fascinating term IoT, unleashes several new problems in security and networking field. In fact, the things which are integrated with each other to form IoT have the common characteristics of low computation power and limited battery power. Accordingly, we have to propose solutions by considering these above mentioned characteristics [4]. Many researchers are involved in developing solutions for the technical requirement of IoT. This research paper gives an overview of the current start of art technology on IoT. More specifically:

[1,2] Banasthali University, Rajasthan, India

[*3,4] Lovely Professional University, Punjab, India

- Discuss the vision of different researcher for IoT.
- A review of the technological benefits of IoT in daily life.
- Present an analysis on the major issues related to IoT, which faced by the research communities.

The main objective of this research paper is to give the readers a clear understanding of what protocols and proposed solutions is already there for IoT. This research papers also discuss the various factors responsible for the growth of IoT and the various limitations or risk factors associated with the same.

This research paper is organized as follow; Section 2 gives an introduction about the different visions of IoT, which are proposed by different researchers and organizations. Section 3 discussed the diverse factors which enable the IoT. Section 4 addressed the various applications, which are benefited in future by the full deployment of the IoT idea. Section 5 focuses on the research issues related to the same such as networking, security and standardization efforts of the services. Conclusion and future development of IoT is discussed in Section 6.

2. VISUALIZATION OF IOT

Manifold definitions of Internet of Things traceable within the research community testify to the strong interest in the IoT issue and to the vivacity of the debates on it. Upon browsing the literature available it is concludes that a reader might face problems in understanding what actually is an IoT, what are various basic concepts associated with IoT and what they really means, what are the technical and social challenges arises during the complete deployment of IoT. Today the obvious fluffiness of the IoT is just because of the given name “Internet of Things”. The given name syntactically composed of two different terms combined together; the first foot forwards pushes us towards the network oriented hallucination of IoT while the second one diverted the focus of reader towards generic objects which has to be integrated into the common framework [4]. These two terms gives the reader a confused vision of IoT i.e. IoT is a framework which is “internet oriented” or “things oriented”.

While defining IoT, researcher have to make sure that the words ‘‘Internet” and ‘‘Things”, is combined together to introduces a disruptive level of innovation into today ICT world. Internet of Things simply means a global network of interconnected things referred as objects as well. In this global network all the heterogeneous objects or things, which are uniquely addressable and communication with each other using defined protocols [5]. The very first concept of IoT is derived on the basis of ‘‘Things oriented” perspective. Radio–Frequency Identification (RFID) tags are the first things which considered for the development of the IoT concept. Firstly, Auto-ID labs targeted the development of IoT [6] and their focus was to develop a global trading network which has improved object visibility i.e. the current status and location of the objects can be easily traced. According to the authors of [7], RFID is their first choice for implementing the concept of IoT due to their low cost and their world wide acceptance. The other atomic components considered for the implementation of IoT are Near Field Communications (NFC) and Wireless Sensor and Actuator Networks (WSAN). The research work carried out by [7] is not the only one, who discussed about the vision of a things oriented network which is far beyond the concept of RFID uses. During Tunis meeting in 2005, United Nations (UN) also talked about the new dawn of IoT, which results in a new era of networks consists of various objects and this will eliminate the human involvement in data exchange through internet [8].

Another IoT vision statement is also proposed by the consortium CASAGRAS [9] in which they also talked about going beyond the RFID centric approach and proposed a global infrastructure. This proposed global infrastructure will create a world, where the humans will communicate with various physical objects through internet. The member of the same focused on developing a world, where the objects can communicate with each other through internet and serves the society. In this sense, IoT becomes the natural enabling

architecture for the deployment of independent federated services and applications, characterized by a high degree of autonomous data capture, event transfer, network connectivity and interoperability. Later, IPSO (IP for Smart Objects) Alliance [9] is also proposed another vision of IoT. The main objective of IPSO is promoting the communication between smart objects around the world by using Internet Protocol (IP). The same claimed that IP stack is suitable for communication between small and battery operated objects as it is a light weight protocol consumes less power. The IPSO alliance guarantees that to make IoT a reality, IP has all the desired qualities to support the implementation of IoT. By reading IPSO whitepapers, it seems that through a wise IP adaptation and by incorporating IEEE 802.15.4 into the IP architecture, in the view of 6LoWPAN [10], the full deployment of the IoT paradigm will be automatically enabled.

The extended vision of IoT is called as "Web of Things" [11]. In this extended vision of IoT, the physical objects are integrated and connected through each other by using the web standards.

3. ENABLING TECHNOLOGIES

The actual implementation of IoT is only possible by integrating the several available technologies into each other. The main objective of this section is to give an overview of the most relevant technologies to IoT and their role in implementation of IoT.

3.1. Sensing, Identifying and Communication technologies

The main vision behind the recent advancement in information and communication technology (ICT) is "Anytime, anywhere, any-media". Wireless technologies played very significant role while achieving the vision and as result of which, today the ratio between radios and humans is approx 1:1 [12]. Now, we are entering into a new era of radio because of the reduction in their size, energy consumption, cost and weight. In this era, radios are integrated into every object. Thus it will add "anything" to the above mentioned vision which leads to the world of IoT. In this context, RFID can be one of the key components for IoT [13]. RFIDs are composed of readers and RFID tags. These RFID tags are identified by unique identifier and these RFID tags are applied to the various objects to communication. Readers trigger the tag transmission by generating an appropriate signal, which represents a query for the possible presence of tags in the surrounding area and for the reception of their IDs. RFID systems are very well used in wide range of real time applications such as healthcare and security, without being actually in line-of-sight. This feature of RFID allows us to connect the real world to the virtual world.

The other key component which also play very important role in the making IoT a reality is Sensor networks. Sensor Networks can be integrated with RFID to better track the status of objects i.e., their location, temperature, movements, etc. Sensor networks are proposed to used into various real time applications such as military applications, habitat or environment monitoring, intelligent transportation

Table 1: Comparison between RFID, WSN and RSN

	Processing	Sensing	Communication	Range (m)	Power	Lifetime	Size	Standard
RFID	No	No	Asymmetric	10	Harvested	indefinite	Very small	ISO 18000
WSN	Yes	Yes	Peer to Peer	100	Battery	<3 years	small	IEEE 802.15.4
RSN	Yes	Yes	Asymmetric	3	Harvested	indefinite	small	None

systems, and industrial plant monitoring. Almost all the commercial wireless sensor network solutions are based on IEEE 802.15.4 standard. This standard defines the physical and MAC layers for low-power, low bit rate communications in wireless personal area networks (WPAN) [14]. IEEE 802.15.4 does not include specifications on the higher layers of the protocol stack, which is necessary for the seamless integration of sensor nodes into the Internet.

Table 1 [4] provides a brief comparison of the various characteristics of RFID systems (RFID), wireless sensor networks (WSN), and RFID sensor networks (RSN) [15]. Following are the observations based on the comparison shown in table 1:

- The RFID systems are very compact and small in size and the lifetime of the RFID system are not dependent of the battery duration.
- Wireless sensor networks provide a wide range of coverage and the mostly the communication is peer to peer.
- RFID sensor networks are the combination of the advantages of the above mentioned systems and used for sensing, computing and for communication.

3.2. Middleware

Middleware can be defined as the software layers punctuate between the technology and the applications associated with the technology. The main objective of middleware is to hide the unnecessary details associated with the technology. In last decade, the concept of middleware is gaining importance because of its nature to simplify the development and integration process of the new service into the legacy application or systems. The most promising middleware architecture proposed for IoT is based on Service Oriented Architectures (SOA) approach. By embracing the SOA approach, decomposing of the complex and monolithic systems or services into very simplified one [16]. SOA doesn't focus on particular one specific technology for the service implementation and as result of which hardware and software reuse it increased, this reuse of the hardware and software will reduce the development cost and time [17]. Figure 1 [4], gives an overview of SOA based architecture for IoT middleware. The shown architecture is focused on objects, object abstraction, service composition and various applications etc.

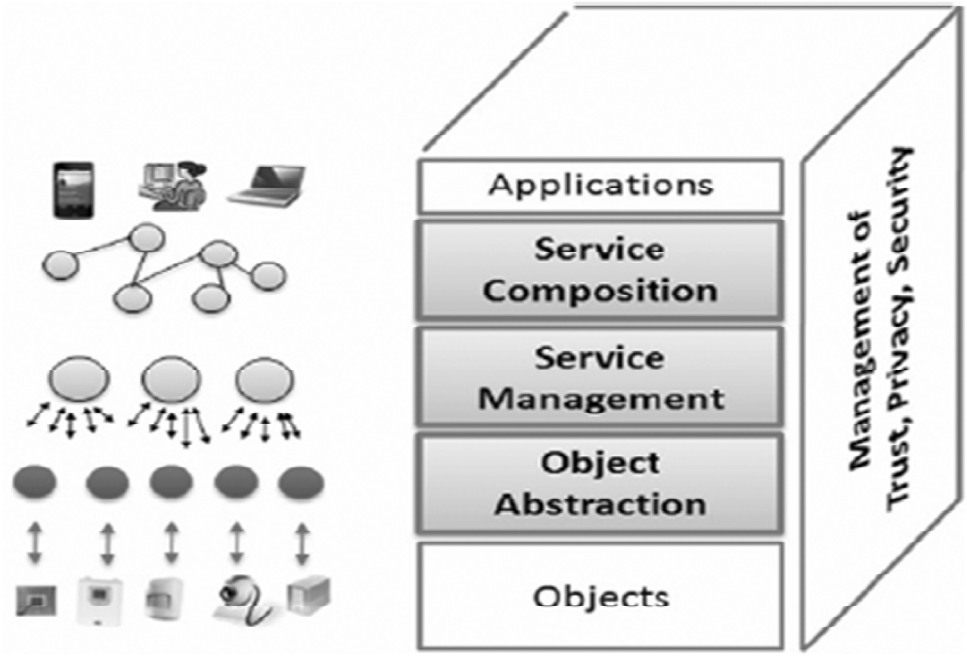

Figure 1: IoT middleware architecture based on SOA

4. APPLICATIONS

The real applications associated with IoT are still unfold because of the wide range of the potentialities offered by IoT. A very small part of the applications are available nowadays and many other significant applications are yet too implemented for the benefit of society. Such applications help us at home, work, gym and travelling etc. The existing applications may be consists of intelligent objects but the communication and information gathering from external environment among these objects are not available. The various applications associated with IoT can be grouped into the following domains and shown in Figure 2:

- Healthcare
- Smart cities and Smart environment
- Personal and social
- Logistics including transportation

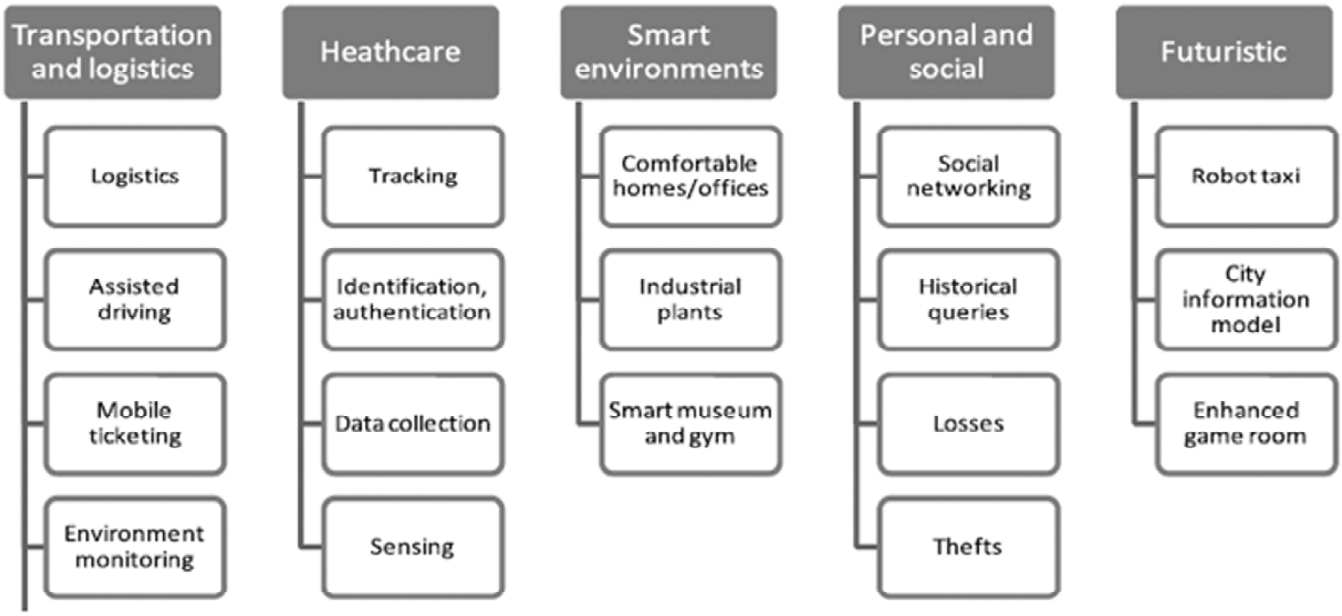

Figure 2: Various application domains related to IoT [4]

5. RESEARCH ISSUES

The various applications which are discussed in section 4, still requires lot of research to make it happen. In this section, we will discuss the research issues which are still open in the field of networking, communication and security related to IoT.

5.1. Standardization of the services or activities

Many researchers and scientific societies are working towards the standardization of IoT activities and some the most relevant are Auto-ID Lab scattered [18, 19], European Standards Organizations (ETSI, CEN, CENELEC, etc.), by their international counterparts (ISO, ITU), and by other standards bodies and consortia (IETF, EPC global, etc.). Table 2 [4], gives brief descriptions of the most relevant standardization of services related to IoT.

5.2. Networking Issues

IoT consist of large number of node and these nodes are used for producing and communicating data irrespective of their positions. This whole scenario requires a very effective addressing mechanism. It is a

Table 2: Description of standardization of services

Standard	Objective	Status	Communication Range (m)	Data Rate (kbps)	Cost ($)
EPC global	Integration of RFID technology into the electronic product code (EPC) framework, which allows for sharing of information related to products.	Advanced	Approx 1	Approx 10^2	.01
GRIFS	European Coordinated Action aimed at defining RFID standards supporting the transition from localized RFID applications to the Internet of Things	Ongoing	Approx 1	Approx 10^2	.01
6LoWPAN	Integration of low-power IEEE 802.15.4 devices into IPv6 networks	Ongoing	Approx 10-100	Approx 10^2	1
ROLL	Definition of routing protocols for heterogeneous low-power and lossy networks	Ongoing	N.S	N.S	N.S
NFC	Definition of a set of protocols for low range and bidirectional communications	Advanced	Approx 10^{-2}	Up to 424	.01
ZigBee	Enabling reliable, cost-effective, low-power, wirelessly networked, monitoring and control products	Advanced	Approx 10-100	Approx 10^2	1

well known fact that, IPv4 addresses is decreasing rapidly and will soon reach zero. Therefore, it is very obvious that we need a different type of addressing mechanism for IoT. As already discussed in table 2, the IPv6 addressing has been proposed for low-power wireless communication nodes within the 6LoWPAN context. Address in IPv6 represented by 128 bits, which means the possible address for the same will be 10^{38}. These possible addresses can be assigned to any objects in IoT. By using IPv6 as addressing scheme in IoT, one of the major networking issues arises in form of integration between the RFID and IPv6. As per the standardization of EPC global regarding RFID, an RFID tag uses 64 to 96 bit identifiers.

Different approaches are proposed [20] [21] [22] [23] regarding the integration of RFID and IPv6 to support the implementation of IoT. In all the proposed approaches the issue of RFID mobility is not considered and assumed that each RFID can be easily accessed through a gateway between the RFID system and network. Now, we can clearly conclude that IoT need appropriate techniques to support the RFID mobility. However, to support the mobility of RFID several solutions were proposed [24] but their validity in IoT scenario is still in doubt as they having some serious issues regarding the scalability and adaptability in harsh heterogeneous environment like IoT. Transport layer supports end-to-end reliability and congestion control and Transmission Control Protocol (TCP) is used as protocol for the communication in traditional internet. According to the requirement of IoT, a new conception of the transport layer is required to support the communication in IoT. Due to the below mentioned reasons, TCP cannot be used as communication protocol in IoT:

- Connection setup: As already discussed, IoT engrosses the small amount of data exchange between physical objects consists of small computational power and limited battery power. TCP is focused on the connection establishment at the starting of each session, which is unnecessary in case of IoT as small amount is to be transferred. The connection setup requires the involvement of end

terminals, which are physical objects in case of IoT having limited battery and computation power [4].

- Congestion control: TCP is also responsible for congestion control during communication but in case of IoT, the objects exchanges very small amount of data with each other in single sessions. Due to the small amount of data exchange between physical objects, the concept of congestion control in IoT is useless, in fact this may cause serious performance issues in IoT. The whole TCP session will be concluded with the transmission of the first segment and the consequent reception of the corresponding acknowledgement [4].
- Data buffering: During communication using TCP, TCP ensure that the data must be buffered at the sender and receiver terminals because at senders end stored data is used in case of data lost and at the receiver side data is stored for order delivery of packets. But in IoT the sender and receiver are the physical objects having very small storage, this storage cannot buffer the data [4].

Another networking issue related to the implementation of IoT is traffic characterization. In IoT, we are not aware about the characteristics of the data which going to be exchanged between physical objects and humans, so it very difficult for us to design the network and protocol infrastructure for IoT. As it is fundamental requirement to know about the traffic characteristics while designing the network infrastructure and protocols. Obviously, this should be just a starting point and specific solutions for the IoT should be introduced in the future.

5.3. Security Issues

Security is one the biggest hurdle for the implementation of IoT. The IoT concept is more vulnerable to the attacks because firstly, In IoT scenario the most of the components are the physical objects which are unattended most of the time and this will result in physical attacks on them. Secondly, the communication in IoT is wireless, which attracts the eavesdropping. Third and the most important issue is that we cannot implement complex and sophisticated security mechanism in IoT as they require more computation and energy efficient devices and we already characterized the IoT devices as low computation and limited battery powered devices [4].

More specifically, the major security issues in IoT are related to the authentication and data integrity. Firstly, to achieve authentication in IoT is very difficult because most of the IoT visions are argued that RFID is the basic technology used for implementation of IoT. The authentication process is very difficult to implement in RFID systems because of the passive RFID tags cannot exchange the number messages required for authentication i.e. cannot exchange some many messages with authentication server. In this context, many security solutions are also proposed for the sensor networks as well [27], we are discussing the security issues in sensor networks because sensor networks are also atomic components of IoT as well. However, the proposed solution scan be applied in the case where the sensor nodes are the part of sensor network and connected to external network for example internet through other nodes such as base station. In IoT concept these sensor nodes are directly connected to the internet or external network as individual and independent nodes so, it is very essentials to authenticate these nodes because they are not belong to a networks, they communicated with each other as independent nodes. In the last few years, some solutions have been proposed for RFID systems; however, they all have serious problems as described in [28].

Finally, on the basis of literature survey conducted for this research work, it has been observed that most the security solutions proposed uses some kind of cryptographic methodologies. These cryptographic algorithms consumes a significant amount of resources such as energy and computation power at both the ends i.e. sender and receiver. These solutions cannot be used for providing security in IoT, as the atomic components used for the IoT are RFID and sensors, which already characterized as devices with limited battery and computation power. IoT requires a new set of solutions to solve the security issues regardless of

the scarcity of resources. Some of the solutions are proposed for marinating the satisfactory level of security in IoT for example light symmetric key cryptographic schemes [33, 34] for RFID systems and sensor network scenarios [27]. However, as we already discussed, key management schemes are still at an early stage (especially in the case of RFID) and require large research efforts.

6. CONCLUSION

The growth in Information and communication technology (ICT) changed our lives and integrated a virtual world into our professional lives as well. IoT has the potential to give a new direction to this by enabling the communication between the physical objects and humans through internet. This will lead us towards our vision of ‘‘anytime, anywhere, any-media, anything” communications. In this research work it has been observed that IoT can be considered a global network but it is significantly different from internet. In this research work, we have studied all the important aspects related to IoT and also explore its future requirement. We have also discussed the research issues which are still open in IoT in terms of standardization, networking and security. Definitely, the current available technologies can form the firm base for making IoT a reality but the current technologies do not exactly fit according to the IoT requirement of scalability and efficiency. We believe that the interest shown by the various industries towards the IoT applications which can use for their purpose open the gates for the research regarding standardization, networking and security.

REFERENCES

[1] Y. Montcheuil, “How to make the most of the Internet of Things,” http://www.itproportal.com/2014/04/25/how-tomake-the-most-of-the-internet-of-things/.

[2] Buckl C, Sommer S, Scholz A, Knoll A, Kemper A, Heuer J, Schmitt A. Services to the field: An approach for resource constrained sensor/actor networks. In Advanced Information Networking and Applications Workshops, 2009. WAINA’09. International Conference on 2009 May 26 (pp. 476-481). IEEE.

[3] Nest labs, “Nest, Smart thermostat system,” 2014.

[4] Atzori L, Iera A, Morabito G. The internet of things: A survey. Computer networks. 2010 Oct 28; 54(15):2787-805.

[5] INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nano systems, in: Co-operation with the Working Group RFID of the ETP EPOSS, Internet of Things in 2020, Roadmap for the Future, Version 1.1, 27 May 2008.

[6] Auto-Id Labs, <http://www.autoidlabs.org/>.

[7] Presser M, Gluhak A. The internet of things: Connecting the real world with the digital world. EURESCOM mess@ ge–The Magazine for Telecom Insiders. 2009;2.

[8] Botterman M. Internet of Things: an early reality of the Future Internet. In Workshop Report, European Commission Information Society and Media 2009 May.

[9] A. Dunkels, J.P. Vasseur, IP for Smart Objects, Internet Protocol for Smart Objects (IPSO) Alliance, White Paper #1, September 2008, <http://www.ipso-alliance.org>.

[10] J. Hui, D. Culler, S. Chakrabarti, 6LoWPAN: Incorporating IEEE 802.15.4 Into the IP Architecture – Internet Protocol for Smart Objects (IPSO) Alliance, White Paper #3.

[11] Guinard D, Trifa V. Towards the web of things: Web mashups for embedded devices. In Workshop on Mashups, Enterprise Mashups and Lightweight Composition on the Web (MEM 2009), in proceedings of WWW (International World Wide Web Conferences), Madrid, Spain 2009 Apr 20 (p. 15).

[12] Srivastava L. Pervasive, ambient, ubiquitous: the magic of radio. In European Commission Conference ‘‘From RFID to the Internet of Things”, Bruxelles, Belgium 2006 Mar.

[13] K. Finkenzeller, RFID Handbook, Wiley, 2003.

[14] Luhach AK, Dwivedi SK, Jha CK. Applying SOA to an E-commerce system and designing a logical security framework for small and medium sized E-commerce based on SOA. In Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on 2014 Dec 18 (pp. 1-6). IEEE.

[15] Buettner M, Greenstein B, Sample A, Smith JR, Wetherall D. Revisiting smart dust with RFID sensor networks. In Proceedings of the 7th ACM Workshop on Hot Topics in Networks (HotNets-VII) 2008 Oct 6.

[16] De Deugd S, Carroll R, Kelly K, Millett B, Ricker J. SODA: service oriented device architecture. IEEE Pervasive Computing. 2006 Jul 1(3):94-6.

[17] Luhach AK, Dwivedi SK, Jha CK. Implementing the Logical Security Framework for E-Commerce Based on Service-Oriented Architecture. In Proceedings of International Conference on ICT for Sustainable Development 2016 (pp. 1-13). Springer Singapore.

[18] Floerkemeier C, Bhattacharyya R, Sarma S. Beyond RFID. Proceedings of TIWDC. 2009.

[19] Sung J, Lopez TS, Kim D. The EPC sensor network for RFID and WSN integration infrastructure. InPervasive Computing and Communications Workshops, 2007. PerCom Workshops' 07. Fifth Annual IEEE International Conference on 2007 Mar 19 (pp. 618-621). IEEE.

[20] Ma YW, Lai CF, Huang YM, Chen JL. Mobile RFID with IPv6 for phone services. InConsumer Electronics, 2009. ISCE'09. IEEE 13th International Symposium on 2009 May 25 (pp. 169-170). IEEE.

[21] Luhach AK, Luhach R. Research and implementation of security framework for small and medium sized e-commerce based on SOA. Journal of Theoretical and Applied Information Technology. 2015 Dec 31;82(3).

[22] Yoon DG, Lee DH, Seo CH, Choi SG. RFID networking mechanism using address management agent. InNetworked Computing and Advanced Information Management, 2008. NCM'08. Fourth International Conference on 2008 Sep 2 (Vol. 1, pp. 617-622). IEEE.

[23] <http://ipv6.com/articles/applications/Using-RFID-and-IPv6.htm>.

[24] Akyildiz IF, Xie J, Mohanty S. A survey of mobility management in next-generation all-IP-based wireless systems. Wireless Communications, IEEE. 2004 Aug;11(4):16-28.

[25] Cerf V, Dalal Y, Sunshine C. Specification of internet transmission control program. INWG General Note; 1974 Dec 1.

[26] Demirkol I, Alagoz F, Deliç H, Ersoy C. Wireless sensor networks for intrusion detection: packet traffic modeling. IEEE Communications Letters. 2006 Jan 1;10(1):22-4.

[27] Eschenauer L, Gligor VD. A key-management scheme for distributed sensor networks. InProceedings of the 9th ACM conference on Computer and communications security 2002 Nov 18 (pp. 41-47). ACM.

[28] Juels A. RFID security and privacy: A research survey. Selected Areas in Communications, IEEE Journal on. 2006 Feb;24(2):381-94.

[29] Acharya R, Asha K. Data integrity and intrusion detection in wireless sensor networks. In Networks, 2008. ICON 2008. 16th IEEE International Conference on 2008 Dec 12 (pp. 1-5). IEEE.

[30] Karygiannis T, Eydt B, Barber G, Bunn L, Phillips T. Guidelines for securing radio frequency identification (RFID) systems. NIST Special publication. 2007 Apr;80:1-54.

[31] Kumar R, Kohler E, Srivastava M. Harbor: software-based memory protection for sensor nodes. InProceedings of the 6th international conference on Information processing in sensor networks 2007 Apr 25 (pp. 340-349). ACM.

[32] Krawczyk H, Canetti R, Bellare M. HMAC: Keyed-hashing for message authentication.

[33] Feldhofer M, Dominikus S, Wolkerstorfer J. Strong authentication for RFID systems using the AES algorithm. InCryptographic Hardware and Embedded Systems-CHES 2004 2004 Aug 11 (pp. 357-370). Springer Berlin Heidelberg.

[34] Calmels B, Canard S, Girault M, Sibert H. Low-cost cryptography for privacy in RFID systems. InSmart Card Research and Advanced Applications 2006 Apr 19 (pp. 237-251). Springer Berlin Heidelberg.

[35] Koponen T, Chawla M, Chun BG, Ermolinskiy A, Kim KH, Shenker S, Stoica I. A data-oriented (and beyond) network architecture. InACM SIGCOMM Computer Communication Review 2007 Aug 27 (Vol. 37, No. 4, pp. 181-192). ACM.