IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Architectural Layers of Internet of Things and Issues at Different Layers

J. Kaur[1*], J. Sengupta[2]

[1,2] Department of Computer Science & Engineering, Punjabi University, Patiala, India

Corresponding Author: jashn00042@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i5.16901694 | Available online at: www.ijcseonline.org

Accepted: 14/May/2019, Published: 31/May/2019

Abstract— IoT is composed of tiny objects implanted with sensors, actuators and Radio Frequency Identification (RFID) tags which make the best use of the network to offer an extensive choice of applications. The major cause for the rapid expansion of IoT is the economic range of intelligent objects and easy availability of internet services. The sensitive information is accessible over network and thus creating threat to data and information. The information privacy is a critical factor in the growth of IoT. In this paper, we review the basics of privacy in IoT, various issues related to privacy and the technologies which can aid in maintain the security of personal data.

***Keywords*—**Privacy , Internet of Things, Identification, Privacy-Preserving Mechanism

I. INTRODUCTION

Internet of things is a system of interconnected intelligent automated devices, or items embedded with distinctive tags also known as unique identifiers (UIDs) and the capability of objects to transfer and access the data/information over network without the need of human control or any other kind of interactions. It is defined as a network with intelligent objects and these smart things share a required information and knowledge by the user over the network. The total Internet of Things (IoT) connected devices installed base is projected to reach 75.44 billion worldwide by 2025, a five times increases in ten years. The use of IoT technology will definitely change the standards of living but at the same time, Data privacy and security are among the major concerns with regard to IoT adoption. Once devices are connected to the Internet, they become vulnerable to large number of attacks like of lack of personal data, information, password leaks, routine activities etc. to possible security breaches [1]. Frequent data leaks from network may raise serious concerns about the standards of information security in today's world. IoT uses machine-readable identification tags to tag our everyday objects. Sensors can be a couple of tags to gather more information about the condition of everyday objects and those around them. The same applies to different companies where computers keep track of stocks and resources available and keep them to optimum levels, thereby saving a lot of time and expenses [2], [3]. However, it is necessary to consider the security and privacy issues. There is a connection between every small thing and communication takes place over Internet, thus it’s very easy to track the engagements, lifestyles and current likings of users, thus giving rise to security and privacy issues. Principles of informed consent, data confidentiality and security must be safeguarded in order to promote a more widespread adoption of IoT-based technologies [4].

The paper is organized as follows, Section I contains the introduction of IoT elements, Section II contains introduction to privacy and brief protocol architectural layers, Section III contains various issues and Section IV concludes research survey with future directions.

II. IOT ELEMENTS

IoT elements have certainly bridge the void from smart cities to smart home by monitoring and controlling all the fields. Consistently there are certain key conditions affecting our selection of components for IoT devices. The IoT elements basically comprises of three major divisions a) Hardware – This includes the sensors, actuators and embedded communication hardware b) Middleware –The storage space , various processing technologies and methodologies[5] for data analysis and c) Presentation - novel easy to have knowledge visually and analyzing the systems. The key IoT elements which play a major role are as following:

A. IDENTIFICATION

Distinct identification (RFID) and low power Nano-scale sensors are the foremost enablers of IoT comprehension through the individuality of ID, tiny size, recognizing, loading and administering capabilities. RFID technology is a chief revolution in the implanted communication model, which permits design of microchips for wireless data communication. They assist in spontaneous identification of anything they are attached to, acting as an automated barcode [4, 5]. The passive RFID labels are not battery fuelled and they utilize the intensity of the reader's cross-examination flag to impart the ID to the RFID reader's. This has brought about numerous applications especially in retail and store network. The applications can be found in transportation (substitution of tickets, enrolment stickers) and access control applications also [5], [6]. The detached labels are presently being utilized in many bankcards and street toll labels which are among the worldwide organizations. Active RFID reader's have their battery supply and can initiate the correspondence. Of the few applications, the principle use of active RFID labels is in port holders [7] for observing contents.

B. SENSING

The important step in IoT workflow is gathering information at a "point of activity." This can be information captured by an appliance, a wearable device, a wall mounted control or any of commonly found devices. The sensing can be biometric, biological, environmental, visual or audible (or all the above). The unique thing in the context of IoT is that the device doing the sensing is not one that typically gathered information in this way. Sensing technology specific to this purpose is required.

The kinds of sensing nodes required for the IoT shift generally is contingent upon the applications included. The sensors could incorporate a camera framework for picture observing, water or gas stream meters for energy saving, radar vision when dynamic security is required, RFID detectors detecting the nearness of an individual, entryways and locks with open/close circuits that show a building interruption or a basic thermometer estimating temperature. These sensor nodes all will convey a unique ID and can be controlled independently by means of a remote order and control topology. Utilize cases exist today in which a cell phone with RFID as well as close field correspondence (NFC) and GPS usefulness can approach individual RFID/NFC-empowered "things" in a building, speak with them and enrol their physical areas on the system. Thus, RFID and NFC will have a place in remote enrolment, and, eventually, direction and control of the IoT.

C. COMMUNICATION

Communication tools join diverse and heterogeneous entities to provide particular aids. A large number of the new IoT gadgets we are seeing today are not intended for ideal correspondence with cloud administrations. IoT gadgets require methods for transmitting the data detected at the gadget level to a Cloud-based administration for consequent handling. This requires either Wi-Fi (remote LAN based interchanges) or WAN (wide zone arrange… i.e. cell) interchanges. Moreover, contingent upon the need of short range correspondence, different abilities may likewise be required. These could incorporate Bluetooth, ZigBee, Near-field or a scope of other short range specialized techniques. For locating, GPS is frequently required. The correspondence conventions accessible for the IoT are: Wi-Fi, Bluetooth, IEEE 802.15.4, Z-wave, LTE-Advanced, Near Field Communication, Ultra-Wide transfer capacity, Low-Power Wide-Area Network and various emerging standards.

D. COMPUTATION

Microcontrollers, microchips, system on chips (SoCs) or field programmable entryway clusters, and programming applications play major role in this module. Accumulated information is transmitted to a cloud based service where the data rolling in from the IoT gadget is collected with other cloud based information to give helpful data to the end client. The information being combined can be data from other web sources and from others buying in with comparable IoT gadgets. Regularly, there will be a few information preparing required to give helpful data that isn't really clear in the crude information. Numerous hardware platforms like Arduino or Raspberry PI are created and different software is also used. The cloud platform is an especially critical computational piece of IoT, since it is amazing in handling different information progressively and in separating a wide range of profitable data from the accumulated information.

E. SERVICES

The services in IoT can be ordered into four classes: character related services, data collection services, synergistic mindful services and pervasive services. Identification related aids establish the framework for different kinds of skills, since each application mapping genuine items into the virtual world needs to distinguish the articles first [10]. Data accumulation services assemble and outline the crude data, which should be handled and detailed. The acquired information is additionally used by the cooperative mindful facilities to settle on choices and respond in like manner. Pervasive assistances are for offering the community mind full service to anybody on interest, anytime and anyplace. [2]

Semantic means the capacity to extract learning wisely in order to give the required assistance. This procedure normally incorporates: finding assets, using assets, demonstrating data, and perceiving and investigating information. The regularly utilized semantic advances are resource description framework, web ontology language, proficient XML exchange, and so forth. [3]

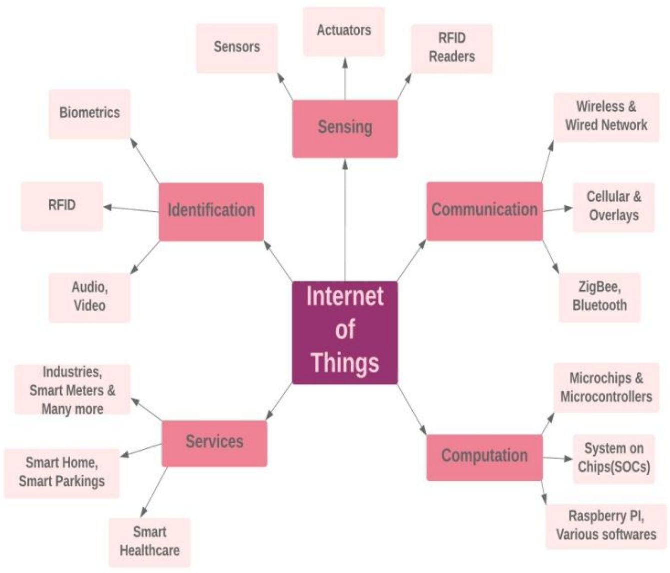


Fig. 1 The Elements of IoT

III. PRIVACY AND DIFFERENT ARCHITECTURAL LAYER

Privacy means to retain the capability of data being secret and is only controlled by the owner and no other user can make any modification/control the data/ communication. Contrasting confidentiality, which is basically encrypting the data without which aims to encrypt the data without being snooped and obstructed by an unauthorized users, privacy guarantees that user is confined to have defined particular controls built on acknowledged facts and no other important knowledge/data can be obtained from the acknowledged facts [10], [12], [16], [20]. Privacy is one of the major safety principles because of its numerous numbers of devices, amenities, and individuals contributing to the similar interaction system in IoT.

The different organizations and service providers define, implement and recognize IoT architecture in different ways. However, the basic architecture of an IoT system remains same underneath every implementation and business model. The basic architecture of an IoT system can be understood from a four-layer model and the four layers are: Identification, Network/Transmission, Management and Application Layer. The brief discussion about the roles of different layers and protocols is as following:

I) IDENTIFICATION LAYER:

It is a lowest level of IoT construction. This is the source of access to information throughout the IoT. In this layer, IOT devices (including sensor networks) and technologies physically connecting co-located devices, or devices to standard internet network, are included. Compared to OSI model, this layer merges physical, data link, and network and transport layers of typical Internet network. On comparing with TCP-IP model, this layer merges physical and network access, Internet and transport layers. Some of the standard protocols defined for physical and network access layers are as follow – Ethernet, Bluetooth Low Energy, Wireless HART, Zigbee, Z-wave, RFID, IEEE 802.11.ah, IEEE 802.15.4e etc. [8] The various issues at this layer include physical security of sensing devices and privacy of information to be collected. IoT cannot provide a perfect security protection system and it is vulnerable to the attack due to diversity, energy limited, and simple and weak protective capability of sensing node, which affects the security of WSN, RFID and M2M terminal. The RFID includes security problems such as information leakage, replay attacks, information tracking, tampering, cloning attacks and man-in-the-middle attacks. Other security issues includes capture gateway node, physical capture, unfair attacks, congestion attack, DoS attacks, node replication attack and forward attack[9].

II) NETWORK LAYER:

This layer is basically responsible for communicating and routing. The used network/Gateways are responsible for routing information obtained from the sensors, and hand it to the upcoming layer called the management layer. The Fig. 2 below gives the brief layout of IoT architecture:

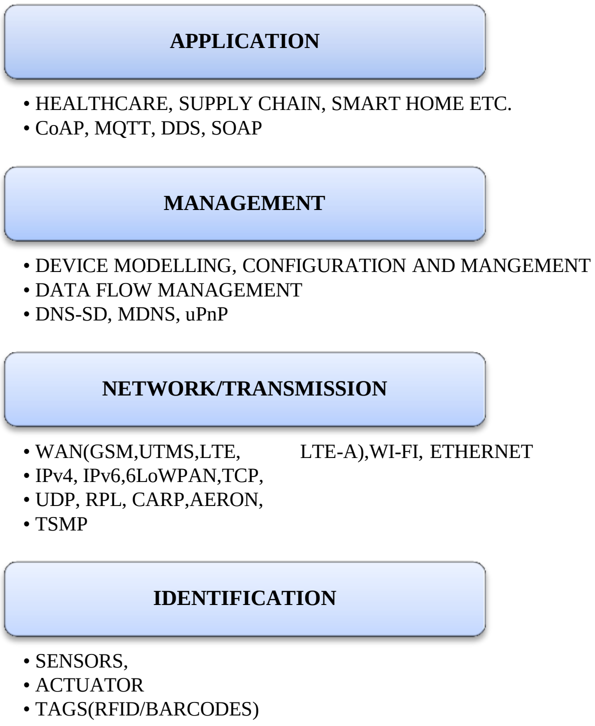


Fig. 2 Architecture Layout IoT and major devices and protocols used.

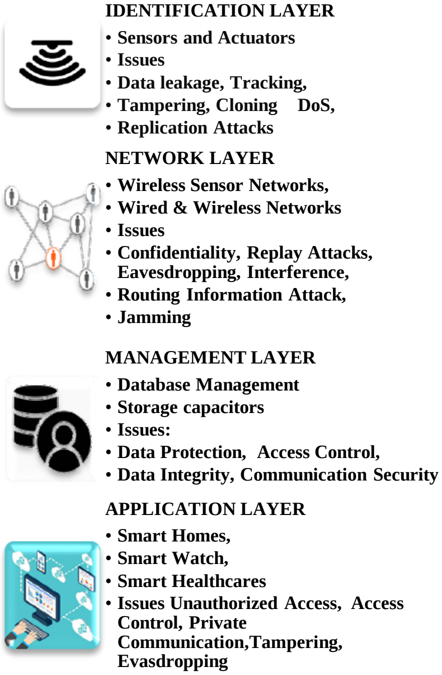
This layer is responsible for addressing of data packets over internet. The incoming data grams contains source and destination addresses. At network layer, the packets are encapsulated with unique addresses, which are called IP addresses. Earlier IPv4 was used for addressing at network layer but its IP addresses have already exhausted. So, a new network layer protocol IPv6 has been specified which would have 128 bit addresses. The IPv6 has address space for 1038 addresses. 6LoWPAN is another network layer protocol for low power wireless personal area networks. It is an IPv6 protocol developed for wireless sensor networks and home area networks. So, the popular network layer protocols are IPv4, IPv6, 6LoWPAN, 6Lo, 6TiSCH, IPv6 over Bluetooth Low Energy, IPv6 over G.9959. This layer also needs to have a good capacity for storage for huge data which is obtained from the sensors, tags etc. To add, there is also a need of reliable trust performance in all networks like private, public, hybrid etc. All the networking protocols integrate on this layer. The major issues at this layer are routing information attack, jamming, confidentiality etc.

III) MANAGEMENT LAYER

The management layer is used for handling the IoT services. It is responsible for safeguarding evaluation of IoT devices, evaluation of information (Stream Analytics, Data Analytics), and device management. Data management is a prerequisite to obtain the essential knowledge from the massive quantity of raw data collected by the sensor devices to generate a valuable calculation of all the data composed. [20]This layer differentiates the IoT networks or cloud networks with typical Internet networks. The IoT devices need to find other devices, services and resources over Internet. So, there is a need for resource management and registration process on cloud networks. For this purpose, service discovery and management protocols are specified. Some of the popular protocols for service discovery on IoT systems are DNS-SD (DNS-Service Discovery), mDNS (Multicast Domain Name System), uPnP, Simple Discovery Service Protocol. Some of the currently available service discovery platforms and technologies are HyperCat, Physical Web, Wi-Fi Aware, Bluetooth Beacons, Shazam, Open Hybrid, Chirp. Also, certain situation requires immediate response to the situation. This layer helps in doing that by abstracting data, extracting information and managing the data flow. [21] This layer is also responsible for data mining, text mining, service analytics etc. The various issues are session attacks, DoS attacks, and unauthorized access.

IV) APPLICATION LAYER

Application layer is the most important in terms of users as it acts as an interface that provides necessary modules to control, and monitor various aspects of the IoT system. Applications allow users to visualize, and analyze the system status at present stage of action, sometimes prediction of futuristic prospects it is responsible for effective utilization of the data collected[20]. Various IoT applications include Home Automation, E-health, and E-Government etc. This layer is implemented through a dedicated application at the device end. It is the browser which implements application layer protocols like HTTP, HTTPS, SMTP and FTP. The diagram below shows enabling technologies below:-



IDENTIFICATION LAYER
- **Sensors and Actuators**
- **Issues**
- **Data leakage, Tracking,**
- **Tampering, Cloning DoS,**
- **Replication Attacks**

NETWORK LAYER
- **Wireless Sensor Networks,**
- **Wired & Wireless Networks**
- **Issues**
- **Confidentiality, Replay Attacks, Eavesdropping, Interference,**
- **Routing Information Attack,**
- **Jamming**

MANAGEMENT LAYER
- **Database Management**
- **Storage capacitors**
- **Issues:**
- **Data Protection, Access Control,**
- **Data Integrity, Communication Security**

APPLICATION LAYER
- **Smart Homes,**
- **Smart Watch,**
- **Smart Healthcares**
- **Issues Unauthorized Access, Access Control, Private Communication,Tampering, Evasdropping**

Fig 3 Enabling Technologies of IoT and Issues at each layer.

Embedding the privacy checks and privacy enhancing Technologies in the devices itself is one of the major features in today's intelligent objects [21]. In Year 2001, six rules were defined in privacy by Design (PbD) by Langheinrich [20] which included notice, choice and consent, proximity and locality, anonymity and pseudonymity, security, and access and recourse. The main use of these rules were there so has to maintain the secrecy and privacy of individuals property or in other case one will ignore the importance of privacy in today's digital world. [17], [21], [22].

IV. CONCLUSION

The prevalent use of wireless network and economical smart objects has lead to the rapid growth of internet of things in today's world. In this paper, we study the privacy and various issues at different layers of Internet of things. The review layered IoT architecture is done and various privacy requirements and solutions have been proposed. To increase the benefits from IoT, the adoption of various privacy and security mechanism needs to be done. We expect that this paper will provide a brief understanding about internet of things and various privacy issues critical for an open adoption for this rapidly emerging technique.

REFERENCES

[1]A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "*Internet of things: A survey on enabling technologies, protocols, and applications*". IEEE Communications Surveys Tutorials, 17(4):2347–2376, Fourth quarter **2015**.

[2] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, *"Internet of things: Security vulnerabilities and challenges*". In Proc. of **2015 IEEE** Symposium on Computers and Communication (ISCC), **July 2015.**

[3]L. Atzori, A. Iera, and G. Morabito, "*The internet of things: A survey"*In **Computer Networks**, 54(15):2787–2805, **October 2010**.

[4]M.V. Bharathi, R. C. Tanguturi, C. Jayakumar, and K. Selvamani., *"Node capture attack in wireless sensor network: A survey*". In Proc. of 2012 IEEE International Conference on Computational Intelligence Computing Research (ICCIC), **December 2012.**

[5]F. Bonomi, R. Milito, J. Zhu, and S. Addepalli*, "Fog computing and its role in the internet of things",* In Proc. of the First Edition of the MCC Workshop on Mobile Cloud Computing, **August 2012**.

[6] C. Bormann, A. P. Castellani, and Z. Shelby, "*Coap: An application protocol for billions of tiny internet nodes".* IEEE Internet Computing, 16(2):**62–67**, **March 2012**.

[7] G. Gan, Z. Lu, and J. Jiang, *"Internet of things security analysis"*, In Proc. of 2011 International Conference on Internet Technology and Applications (iTAP), **August 2011**.

[8] M. Leo, F. Battisti, M. Carli, and A. Neri*, "A federated architecture approach for internet of things security"*, In Proc. of 2014 Euro Med Telco Conference (EMTC), **November 2014.**

[9] Y. Liu and G. Zhou, *"Key technologies and applications of internet of things"*, In Proc. of 2012 Fifth International Conference on Intelligent Computation Technology and Automation (ICICTA**), January 2012**.

[10] P. Lpez, D. Fernndez, A. J. Jara, and A. F. Skarmeta, *"Survey of internet of things technologies for clinical environments*", In Proc. of 2013 27th International Conference on Advanced Information Networking and Applications Workshops (WAINA), **March 2013.**

[11] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, *"Internet of things (iot) security: Current status, challenges and prospective measures*", In Proc. of 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), **December 2015**.

[12] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things", in Ad Hoc Networks, 10(7):**1497–1516**, **September 2012**.

[13] M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, *"A review on internet of things (iot), internet of everything (ioe) and internet of nano things (iont)"* In Proc. of 2015 Internet Technologies and Applications (ITA),**September 2015**.

[14] K. P. N. Puttaswamy, R. Bhagwan, and V. N. Padmanabhan, "**Anonygator: Privacy and integrity preserving data aggregation",** In Proc. of the ACM/IFIP/USENIX 11th International Conference on Middleware, Middleware '10, Berlin, Heidelberg, **December 2010, Springer-Verlag.**

[15] F. Qiu, F. Wu, and G. Chen, *"Privacy and quality preserving multimedia data aggregation for participatory sensing systems"* in IEEE Transactions on Mobile Computing, 14(6):**1287–1300**, **June 2015.**

[16] X. Ren, X. Yang, J. Lin, Q. Yang, and W. Yu, *"On scaling perturbation based privacy-preserving schemes in smart metering systems"*, In Proc. of 2013 22nd International Conference on Computer Communication and Networks (ICCCN), **July 2013**.

[17] J. A. Stankovic, "*Research directions for the internet of things*". IEEE Internet of Things Journal, 1(1):**3–9**, **February 2014**

[18] K. Zhao and L. Ge., *"A survey on the internet of things security"*, In Proc. of 2013 9th International Conference on Computational Intelligence and Security (CIS), **December 2013**.

[19] G.D'Acquisto, J.Domingo-Ferrer, P. Kikiras, V. Torra, Y.-A. De Montjoye, and A. Bourka, *"Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics,"* arXiv preprint arXiv: 1512.06000**, 2015**

[20] M. Langheinrich, *"Privacy by design principles of privacy-aware ubiquitous systems,"* in Ubicomp 2001: Ubiquitous Computing., pp. **273–291**. Springer**, 2001**

[21] S. Spiekermann and L. F. Cranor, *"Engineering privacy,*" IEEE Transactions on software engineering, **vol. 35**, **no. 1**, pp. **67–82**, **2009.**

[22] S. Lahlou, M. Langheinrich, and C. R¨ocker,*"Privacy and trust issues with invisible computers,"* Communications of the ACM, **vol. 48**, no. 3, pp**. 59–60, 2005**.

[23] V. Tiwari, P. Adkar, *"Implementation of IoT in Home Automation using Andriod Application",* International Journal of Scientific Research in Computer Science and Engineering, Vol**. 7**, Issue **2**, pp. **11-16**, April **2019**.

[24] P. Bhatt, B. Thaker, N. Shah, *"A Survey on Developing Secure IoT Products"*, International Journal of Scientific Research in Computer Science and Engineering, Vol. **6**, Issue **5**, pp. **41**-**44**, October **2018**.

[25] G. Kaur, M.Sohal, *"IOT Survey: The Phase Changer in Healthcare Industry*", International Journal of Scientific Research in Network Security and Communication, Volume-**6**, Issue-**2**, pp. April **2018**.

[26] R. Maruthaveni, V. Kathiresan,*"A Critical Study on RFID"* International Journal of Scientific Research in Network Security and Communication, Volume-**6**, Issue-**2**, pp.62-**65**, April **2018**.

Authors Profile

Ms. Jashanpreet Kaur graduated with Bachelor of Technology from Punjab Technical University, Jallandhar in 2010 and Master of Technology from Punjabi University in year 2012. She is currently pursuing Ph.D. (Faculty of Computational Sciences), Department of Computer Science and Engineering, Punjabi University, Punjab since 2015. She has published 6 research papers in reputed international journals and conferences including IEEE. Her main research work focuses on networking, Network Security, Internet of things and Privacy. She has 3 years of teaching experience.

Dr. Jyotsna Sengupta is a Dean, Research Department at Punjabi University, Patiala, Punjab, India.She is Professor in Department of Computer Science and Engineering. She earned her Ph.D. degree in Computer Science and Engineering from Thapar University, Patiala, Punjab, India, MS degree in Computer Science and Engineering from Santa Clara University, Santa Clara, California, U.S.A., and Bachelor's of Engineering degree in Electronics and Communications from Thapar University, Patiala, Punjab, India. She has published more than 90 research papers in various International and National Conferences and Journals. She has authored two books and edited one book. She is a member of IEEE and the editor of many international journals. Her current research interests include Distributed Systems, Mobile Networks, Cloud Computing and Network Security ad privacy. She has more than 30 years of Teaching and Research experience.