Volume 5, Issue 4, 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security Issues in Internet of Things (IoT): A Survey

Ashvini Balte[*], Asmita Kashid, Balaji Patil
Computer Engineering &MIT Pune,
Maharashtra, India

Abstract— In the recent years, people need to use Internet at anytime and anywhere. Internet of Things (IOT) allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service. IOT can be distinguished by various technologies, which provide the creative services in different application domains. This implies that there are various challenges present while deploying IOT. The traditional security services are not directly applied on IOT due to different communication stacks and various standards. So flexible security mechanisms are need to be invented, which deal with the security threats in such dynamic environment of IOT. In this survey we present the various research challenges with their respective solutions. Also, some open issues are discovered and some hints for further research direction are advocated.

Keywords— Internet-of-Things; Sensor Networks; Smart objects; Sensors; Actuators; ubiquitous; Security

I. INTRODUCTION

In the recent years, Internet has become the most important thing in people's life. Around two billions people around the world use Internet for sending and receiving emails, using social networking applications, sharing large amount of data, playing games and many other things. As the use of Internet is growing day-by-day, another big area is emerging to use Internet as a global platform for allowing the machines and smart objects to communicate, compute and coordinate, called Internet of things (IoT). IoT is a technology where objects around us will be able to connect to each other (e.g. machine to machine) and communicate via the Internet. With the growth of this area, it is not required to sit at a place and access the Internet. Instead, Internet will be accessed from anywhere and from any device. Of course, Internet will remain as a backbone of this new area. IoT will create a world where all the objects, also called smart objects, around us are connected to the Internet and communicate with each other with minimum human intervention [1]

The motivation behind IoT is to create, Smart city [2], to optimize use of public resources, increase the quality of services offered to people and decrease the operational costs of the services. The ultimate goal is to create 'a better world for human beings', where objects around us know what we like, what we want and what we need and act accordingly without explicit instructions [1]

The term IoT is used to refer (i) the global network which interconnects smart objects by using Internet technologies (ii) set of supporting technologies such as Radio Frequency Identifications(RFIDs), sensor/actuators, machine-to-machine communicating devices etc. (iii) combination of application and services using such technologies for business purposes [3]

The IoT depends upon three building blocks, based on the ability of smart objects to: (i) be identifiable (anything identifies itself), (ii) to communicate (anything communicates) and (iii) to interact (anything interacts). The focus of IoT is on the data and information, rather than point-to-point communication.

The major challenges while building IoT involve:

(i) Devices heterogeneity: As IoT is about connecting several smart devices, connecting heterogeneous devices is major challenge while building IoT. Such devices run on different platforms, they uses different protocols to communicate. So it is necessary to do unification of such devices.

(ii) Scalability: Another major challenge is the scalability of the IoT, as everyday new devices/objects are getting connected with the network. It involves issues like addressing/naming conventions, information management, service management etc.

(iii) Ubiquitous data exchange through wireless technologies: In IoT, wireless technologies are used to connect smart devices. It involves issues like availability, network delays, congestion etc.

(iv) Energy-optimized solutions: This is major constraint of IoT. As many devices are connected via networks, energy spent for data communication will be high. The challenge is to optimize the use of energy required for communication between different devices.

(v) Localization and tracking capabilities: The smart objects must be identified and tracking of them is necessary.

(vi) Self-organization capabilities: In IoT, it is required that the smart objects should sense the environment and autonomously react to real world situations, without much human intervention.

(vii) Semantic interoperability and data management: IoT exchange data among different smart objects, it is required that there should be a standardized format for data exchange in order to ensure the interoperability among applications.

(viii) Embedded Security and privacy-preserving mechanisms: In Iot, security and privacy are the major issues in order to get acceptance from users. IoT technology should be secure and privacy-preserving by design.

Main aim of this paper is to present detailed information about the security issues in IoT. The rest of the paper is organized as follows: section II describes literature review in the area IoT. Section III describes Definitions and elements of IOT. Section IV gives security issues related to IOT. Section V presents conclusions and future research directions.

II. Related Work

The basic definitions, trends and elements of IoT are presented in [4]. This paper depicts different definitions given by different researches of IoT. This paper also presents applications of IoT and the areas which are impacted by IoT. Also the future research directions related to IoT technology are mentioned. [3] presents different challenging issues while building an IoT. This paper also discusses about the security issues in IoT. Another advantage of this paper is, it describes the on-going projects related to IoT. This paper states that the security in IoT comprises of data confidentiality, privacy and trust.

The paper [1] describes how the context aware computing is useful for IoT. Context aware computing has proven to be successful in understanding sensor data. This paper presents the basic terminology in context aware computing and also shows how this can be applicable to IoT. The survey presented in this paper includes techniques, methods, models, applications, systems, functionalities and middleware solutions related to context awareness and IoT.

[2] describes how IoT can be used for creating Smart City, where the use of public resources are optimized. [5] describes different security challenges in Smart City. This paper describes the security issues when different devices are connected using Internet (IoT).

[6] describes design, implementation and evaluation of an intrusion detection system, called SVELTE, for IoT.

III. Definitions and Elements

A. *Definitions*

Many definitions of IoT are presented by different researchers. Some of the definitions are presented below:

- Definition by RFID group - The worldwide network of interconnected objects uniquely addressable based on standard communication protocols
- Definition by [6] - Interconnection of sensing and actuating devices providing the ability to share information across platforms through an unified framework. Developing a common operating picture for enabling innovative applications.
- Definition by [1]: The semantic origin of the expression, Internet of Things, is composed by two words and concepts: Internet and Thing, Where Internet can be defined as the world-wide network of interconnected computer networks, based on a standard communication protocol, the Internet suite (TCP/IP), while Thing is an object not precisely identifiable. Therefore, semantically, Internet of Things means a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols.
- Definition by [1]: The Internet of Things allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service.

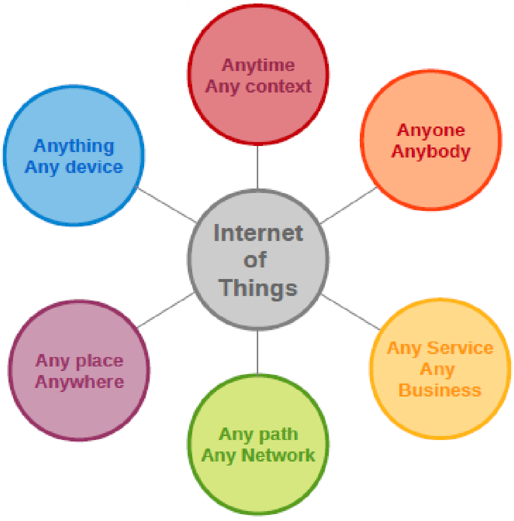

Fig. 1 Definition of IoT by [1]

B. *IoT Elements[6]:*

- *Radio Frequency Identification (RFID):* This technology is used in embedded communication, for designing of microchips for wireless data communication.
- *Wireless Sensor Networks (WSN):* These are efficient, low cost, low power devices useful in remote sensing applications.
- *Addressing Schemes:* Addressing schemes are useful to uniquely identify the 'Things' i.e. smart objects.

- *Data Storage and analytics:* IoT deals with sharing and storing of large amount of data. The data have to be stored and used intelligently for smart monitoring and actuation.
- *Visualization:* This allows interaction of the user with the environment. Extraction of meaningful information from raw data is non-trivial.

IV. SECURITY ISSUES IN IOT

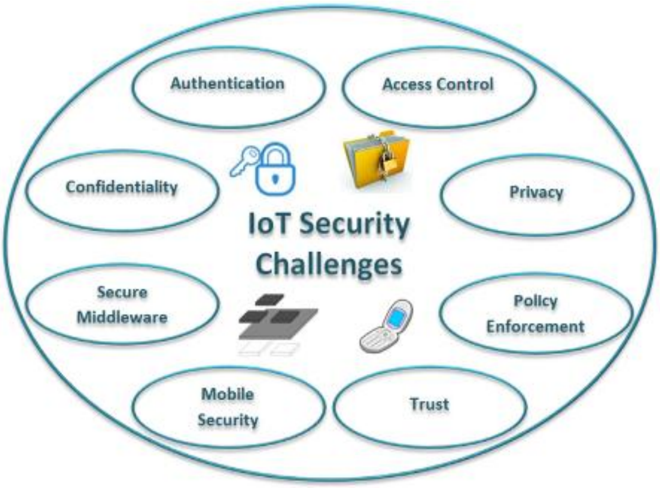

Fig. 2. Major security issues in IoT [7].

As mentioned in section 1 of this paper, there are many challenges involved while building IoT. In this section, major security related challenges while building IoT are described in brief.

A. Access Control

Access control deals with access rights given to the things/devices in IoT environment. In traditional database systems, processing of discrete data is done, however in IoT, processing of flowing data is done. Two terminologies are described for Access Control [8]: 1) data holders (Users), who send/receive data to things. They must send data to authenticated things 2) data collectors (things), which must authenticate users. [9] presents an identity based system for personal location in emergency situation. Authentication problem for outsourced data stream is found in [10]. Access control of streaming data is specified in [11]. Some of the challenges related to Access Control in IoT context involve: How to handle the huge amount of transmitted data (i.e., in the form of stream data) in a common recognized representation? How to support the identification of entities?

B. Privacy

A data tagging for managing privacy in IoT is proposed in [12]. A user-controlled privacy-preserved access control protocol, based on k-anonymity privacy model is proposed in [13]. [14] defines k-anonymity model by changing quasi-identifiers to preserve sensitive data. The privacy risk that occurs when astatic domain name is assigned to a specified IoT node is analysed in [15]. Only some of the privacy issues related to IoT are covered in recent work, there is still a large scope to create privacy preserving mechanisms in IoT context.

C. Policy Enforcement

Policy enforcement implies to the approaches used to cause the application of a set of defined efforts in a system. Policies are performing rules which desire to be acted for the purpose of acknowledging order, security, and consistency on data. Only few works from literature describe how to control policies enforcement. Except for the work in [16], there are no definite solutions for IoT capable to assurance the enforcement of security also privacy policies, although they are essential to assure a safe contribution of IoT prototype. Note that it is important to detect the enforcement mechanisms admissible for the definite IoT context, locating an equilibrium between the assurance of security and privacy issues and the computing efforts demanded by the committed mechanisms themselves. several efforts have already been accomplished to define the conventional languages for the specification of privacy policies, although an approved version of the language which can be applied to IoT paradigm is still insufficient.

D. Trust

The trust idea is used in different contexts and with different explanations. Trust is a complicated concept about which no explanatory acquiescence endures in the scientific literature, [7] furthermore its importance is dimensionally identified. A core problem with many applications towards trust description is that they do not contribute themselves to the demonstration of metrics and computation methodologies. The gratification of trust constraints are exactly related to the identity negotiation and access control effects.

The following issues are still open in IoT-Trust environment:

The introduction of well-defined trust negotiation language, trust negotiation mechanism for data stream access control.

E. Mobile Security

Mobile Mobile nodes in IoT frequently move from one cluster to another, in which cryptography based protocols are used to allow expeditious identification, authentication, and privacy protection. An ad hoc protocol is demonstrated in [17] which is useful when a mobile node joins a new cluster. This protocol also accommodates a valid demand message and an answer authentication message, which speedily implements identification, authentication, and privacy protection. It will be useful to safeguard against replay attack, eavesdropping, and tracking or location privacy attacks. In contrast with other similar protocols such as basic hash protocol, it has less communication overhead, more secure and provides more privacy protection.

TABLE I. CONTRIBUTION OF ONGOING EUROPEAN PROJECTS ON IOT SECURITY

	Project Names								
IOT Security	Butler [26]	EBBITS [27]	Hydra [28]	uTRUSTit [29]	iCore [30]	HACMS [31]	NSF [32]	FIRE [33,34]	EUJapan [35]
Access Control	✓	✓		✓	✓	✓	✓	✓	
Privacy	✓				✓		✓	✓	✓
Enforcement									
Trust				✓	✓		✓		
Mobile	✓						✓		
Middleware		✓	✓		✓				
Confidentiality	✓	✓	✓		✓	✓	✓	✓	✓
Authentication	✓			✓	✓	✓	✓	✓	

Summarizing, also if the security issues of mobile devices (i.e., devices identification and authentication, key and credential storage and exchange) are under investigation by the scientific community, the available solutions partially address these needs, thus requiring further efforts in order to allow the integration with the other IoT technologies.

F. Secure Middleware

With many different technologies are in place within the IoT bench mark, numerous types of middleware layer are also engaged to effect the integration and the security of devices and data within the identical information network. Within alike middlewares, data required to have exact protection constraints. Additionally, in middleware design and development, the different communication mediums for wide scale IoT deployments need to be considered. While many smart devices can natively support IPv6 communications [18, 19], continuing deployments might not acknowledge the IP protocol within the local area scope. So ad hoc gateways are used along with middlewares [20].

Additionally, middlewares immediately lack an accomplished inspection, adopt to arguing to all the IoT conditions, coupled in terms of security and privacy and network behavior. Also, interoperability is becoming an elementary challenge, in order to allocate an individual construction of separated elements, able to co-act and collaborate with each other and as well as to deal data on the basis of standards. IoT includes not only individual data provided by devices/machines, but also by consumers, adjoining the interactions are machine-to-machine and furthermore among consumers and machines additionally among users and users. Therefore, the design and establishment of a middleware adhere an impact on the system composition (i.e., scalability, coupling among components).

G. Authentication & Confidentiality

Different works, describe different protocols and mechanisms to deal with authentication of a user and confidentiality of data in the context of IoT. Some of the major works related to authentication and confidentiality in IoT are as follows: [21] presents smart business security IoT application Protocol, which combines cross-platform communications with encryption, signature, and authentication, in order to improve IoT applications development capabilities. [22] specifies the implementation of two-way authentication security scheme for IoT. As far as confidentiality and integrity is concerned, in [23], it is studied that how the existing key management systems can be applied in the context of IoT. In [24, 25] Public Key Infrastructure (PKI) framework is built for IoT. All these current works are based on solving the problem of lightweight cyphering in pervasive environments. More work needs to be done to create standardized protocols for authentication and Confidentiality in IoT.

V. CONCLUSION AND FUTURE WORK

IoT is the next step towards using Internet Anywhere and Anytime. IoT allows to connect people and devices (things) Anytime, Anyplace, with Anything and Anyone. This paper presents a brief idea about IoT and need of security in IoT. The main security issues related to IoT are explained in brief. TABLE I describes the current ongoing projects in the field of IOT. By observation, it is easy to understand that there is no project still in work which satisfies all security issues in IOT. Also there is no single project which provides policy enforcement in the IOT. In summary, an accomplished vision admiring the assurance of security and privacy constraints in a dissimilar environment, which implies that current security services are insufficient for such contradictory technologies and communication standard. As IoT deals with interconnecting various heterogeneous things, currently there are many challenges occurring while building it. So this area has many open research issues. The future research directions mainly consists of how to deal with the challenges, may be related to security issues, faced by IoT. We hope this paper will be helpful in order to allow a valuable deployment of IoT systems and in suggesting the future research direction.

REFERENCES

[1] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, “Context aware computing for the Internet of Things: a survey,” *IEEE Communications Surveys & Tutorials*, submitted 2013.

[2] A. Zanella, N. Bui, A. P. Castellani, L. Vangelista, and M. Zorzi, “Internet of Things for smart cities*,” IEEE Internet Things* J., vol. 1, no. 1, pp. 22–32, Feb. 2014.

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

[4] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Future Generation Computer Systems*, vol.29, no.7, pp. 1645–1660, 2013.

[5] A. S. Elmaghraby and M. M. Losavio, “Cyber security challenges in Smart Cities: Safety, security and privacy,” *J. Adv. Res*., vol. 5, no. 4, pp. 491–497, Jul. 2014.

[6] S. Raza, L.Wallgren, and T. Voigt, “SVELTE: Real-Time Intrusion Detection in the InternetofThings”, *Ad Hoc Networks*, Elsevier, pp 2661–2674, May 2013.

[7] S. Sicari, A. Rizzardi, L.A Grieco and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead*”, Comput. Netw*. 76, 146–164, 2015,

[8] A. Alcaide, E. Palomar, J. Montero-Castillo and A. Ribagorda, “Anonymous authentication for privacy-preserving iot targetdriven applications”, *Comput. Secur*. 37, 111–123, 2013.

[9] C. Hu, J. Zhan and, Q. Wen “An identity-based personal location system with protected privacy” in IoT, in: *Proceedings - 2011 4th IEEE International Conference on Broadband Network and Multimedia Technology*, IC-BNMT 2011, Shenzhen, China, 2011, pp. 192–195.

[10] S. Papadopoulos, Y. Yang and D. Papadias, “Cads: continuous authentication on data streams”, *in: Proceedings of the 33rd International Conference on Very Large Data Bases*, VLDB ’07,Vienna, Austria, 2007, pp. 135–146.

[11] B. Carminati, E. Ferrari and K.L. Tan, “Specifying access control policies on data streams”, *in: Proceedings of the Database System for Advanced Applications Conference*, DASFAA 2007, Bangkok, Thailand, 2007, pp. 410–421.

[12] D. Evans and D. Eyers, “Efficient data tagging for managing privacy in the internet of things*”, in: Proceedings – 2012 IEEE Int. Conf. on Green Computing and Communications, GreenCom 2012, Conf. on Internet of Things, iThings 2012 and Conf. on Cyber, Physical and Social Computing, CPSCom 2012, Besancon*, France, 2012, pp. 244–248.

[13] X. Huang, R. Fu, B. Chen, T. Zhang and A. Roscoe, “User interactive internet of things privacy preserved access control”, *in: 7th International Conference for Internet Technology and Secured Transactions, ICITST 2012*, London, United Kingdom, 2012, pp.597–602.

[14] J. Cao, B. Carminati, E. Ferrari and K.L. Tan, “CASTLE: continuously anonymizing data streams*”, IEEE Trans. Dependable Secure Comput*. 8 (3) (2011) 337–352.

[15] Y. Wang andQ. Wen, “A privacy enhanced dns scheme for the internet of things”, *in: IET International Conference on Communication Technology and Application*, ICCTA 2011, Beijing, China, 2011, pp.699–702

[16] R. Neisse, G. Steri and G. Baldini, “Enforcement of security policy rules for the internet of things”, *in: Proc. of IEEE WiMob*, Larnaca, Cyprus, pp. 120–127, 2014.

[17] J. Mao and L. Wang, “Rapid identification authentication protocol for mobile nodes in internet of things with privacy protection”, *J. Networks* 7 (7), 1099–1105, 2012.

[18] M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia and M. Dohler, “Standardized protocol stack for the internet of (important) things”, *IEEE Commun. Surv*. Tutorials 15 (3), pp. 1389–1406, 2013.

[19] I. Bagci, S. Raza, T. Chung , U. Roedig and T. Voigt, “Combined secure storage and communication for the internet of things”, in: *2013 IEEE International Conference on Sensing, Communications and Networking*, SECON 2013, New Orleans, LA, United States, pp. 523–631, 2013.

[20] D. Boswarthick, O. Elloumi and O. Hersent, “M2M Communications: A Systems Approach”, first ed., Wiley Publishing, 2012.

[21] Y. Zhao, “Research on data security technology in internet of things”, *in: 2013 2nd International Conference on Mechatronics and Control Engineering*, ICMCE 2013, Dalian, China, 2013, pp. 1752–1755.

[22] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig and G. Carle, “Dtls based security and two-way authentication for the internet of things*”, Ad Hoc Netw. 11* (8) (2013) 2710–2723.

[23] R. Roman, C. Alcaraz, J. Lopez and N. Sklavos, “Key management systems for sensor networks in the context of the internet of things”, *Comput. Electrical Eng.* 37 (2) (2011) 147–159.

[24] W. Du, J. Deng, Y. Han, P. Varshney, J. Katz and A. Khalili, “A pairwise key predistribution scheme for wireless sensor networks”, *ACM Trans*. Inf. Syst. Secur. (TISSEC) 8 (2) (2005) 228–258.

[25] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks", in*: CCS '03 Proceedings of the 10th ACM Conference on Computer and Communications Security*, Washington, DC, USA, 2003, pp. 52–61.
[26] BUTLER Project. <http://www.iot-butler.eu>.
[27] European FP7 IoT@Work project. <http://iot-at-work.eu>.
[28] HYDRA Project. <http://www.hydramiddleware.eu/>.
[29] Usable Trust in the Internet of Things. <http://www.utrustit.eu/>.
[30] iCORE Project. <http://www.iot-icore.eu>.
[31] HACMS Project. <http://www.defenseone.com/technology>.
[32] National Science Foundation Project. <http://www.nsf.gov>.
[33] FIRE EU-China Project. <http://www.euchina-fire.eu/>.
[34] FIRE EU-Korea Project. <http://eukorea-fire.eu/>.
[35] EU-Japan Project. <http://www.eurojapan-ict.org/>.