Security Issues in Internet of Things (IoT)-Enabled Systems: Problem and Prospects

Ajeet S. Poonia, C. Banerjee, Arpita Banerjee and S. K. Sharma

Abstract The use of Internet of things (IoT) devices has enabled the system and their setup to move beyond their respective domains to facilitate better communication, analysis and control. In the future, almost all the industries and organizations working world over will have a setup of IoT devices to contend and remain unchallenged winner in this competitive environment. With technological advancements, there is always possibility of threats and attacks from the outer world and the inside world. The same is true for IoT-enabled systems and a lot of security issues have emerged which poses challenges to the uninterrupted working of the system. The research paper focuses on the various security issues of IoT-enabled systems in general and the challenges it throws to the system. The paper also suggests prospective mitigation mechanism to be adopted from a technical as well as management point of view. The paper concludes with highlighting of the future research directions which may be carried out by the researcher working in this area.

Keywords Security · IoT · IoT devices · IoT-enabled systems · Perspective of IoT systems

A. S. Poonia
Department of CSE, Government College Of Engineering and Technology, Bikaner, India
e-mail: pooniaji@gmail.com

C. Banerjee (✉)
Amity Institute of Information Technology, Amity University Rajasthan, Jaipur, India
e-mail: chitreshh@yahoo.com

A. Banerjee
Department of Computer Science, St. Xavier's College, Jaipur, India
e-mail: arpitaa.banerji@gmail.com

S. K. Sharma
Department of Engineering and Technology, Modern Institute of Technology and Research Centre, Alwar, India
e-mail: sharmasatyendra_03@rediffmail.com

M. Pant et al. (eds.), *Soft Computing: Theories and Applications*,
Advances in Intelligent Systems and Computing 1053,
https://doi.org/10.1007/978-981-15-0751-9_130

1 Introduction

Internet of things (IoT) is a sub area of Information Communication and Technology field which has evolved over time with some massive transformation and probably will continue with the emergence of the future enabling technologies [1]. IoT technology enables the society to envision a world consisting of millions and billions of objects all connected together over public or private Internet Protocol (IP) network and which can sense, communicate, and share information. The main aim of the IoT technology is to monitor, administer, process, and control all smart systems [2].

Irrespective of the nature of business carried out around the globe in the future, all the industries and organizations will have to synchronize their business, technical, operational, etc., processes in order to contend in the competitive environment to survive and continue with its operations [3]. Even a common man in the society will be impacted by the role of IoT technologies and his survival will solely depend upon its proper use [1].

IoT technology is more of a facilitator among various objects and the connection between these objects opens up much vulnerability which may be exploited by any attacker for the malicious intents [4]. Such attacks may be initiated by the outside world as well as the insider [5, 6]. Hence, implementation of IoT technology not only acts as a facilitator but also opens up avenue for the potential attacker to harm the said system thus posing many security issues and challenges which needs to be addressed in a comprehensive manner [7].

First of all, the systems which are to be enabled by the IoT technology should be designed and developed using some foundational security rules [8] backed by some security standards [9]. Some sound mitigation mechanism needs to be devised and in place according to the type of system facilitated by IoT technology which may work from technical as well as managerial perspective as far as safeguarding the system is concerned [10, 11]. The research paper tries to highlight the security aspect of IoT-enabled systems.

The rest of the paper is organized as: Sect. 2 focuses on the security issues and challenges of the IoT-enabled systems, Sect. 3 proposes mitigation mechanism for such IoT-enabled systems from technical point of view, covers the managerial aspect ad proposed mitigation mechanism for IoT-enabled systems, and Sect. 4 provides the conclusion and the future research directions.

2 Security Issues and Challenges of IoT-Enabled Systems

This section deals with the various security issues and challenges of IoT-enabled systems as follows:

Smart Healthcare IoT technology can be applied to healthcare sector for collection and management of patient information systems and related healthcare systems especially for monitoring and control purpose. Body sensor network (BSN) technology

is a very common IoT technology which may be used for the above-said purpose but it opens up avenues for the hacker to get control of the privacy of the patient thereby making them vulnerable for all sorts of exploitations [11].

Smart City The concept of smart city has been designed to provide intelligent services to the local residents and the travelers in forms of smart transportation, smart healthcare, smart environment, smart entertainment, smart energy, etc. Here, the issue of security may be of grave concern as the information collected for providing services not only includes private information of people like resident or traveler but the same technology also controls the facilities. Apart from compromising the privacy of people, the malicious user may also try to manipulate and jeopardize the whole working of system(s) providing intelligent services [12].

Smart Agriculture Smart agriculture is a very major area where IoT technology is employed for mass production of quality crop to meet the growing demand of the global population. Security should form an essential component in the architecture of smart agriculture. In such smart systems, the malicious user may take control of the IoT devices to provide harm to the crop production and in extreme cases may use these devices to inject some harmful or poisonous chemical which may be consumed by millions of people resulting in a devastating situation of mass murder. So ensuring food security should be of utmost concern while implementing IoT technology in the field of agriculture [13].

Smart Cars A connected car offers various information services and entertainment services inside the car because of the addition of the network connection function as a connection between a device inside the car and an outside network. Smart cars use IoT technology to provide various information services and entertainment services to the car user using a network connection between the device present inside the car and the network present in the outside world. This connection may open up many vulnerable spots which can be manipulated and controlled by the hacker and which can expose the smart car to many safety accidents [14].

Smart Home Smart home concept enables a user to have automated system to make their life more easy and safe using various IoT devices and technology. In this concept, the user sitting in any corner of the world is able to monitor and control the various home appliances using mobile or other electronic devices. If these devices or the network connection is compromised by a malicious user, then it may provide harm to the entire home automated system [12].

3 Proposed Mitigation Mechanism—Technical Perspective and Managerial Perspective

This section showcase the proposed mitigation mechanism which may be employed in an IoT-enabled systems to safeguard the system from malicious attack thereby minimizing the harm caused to the said system:

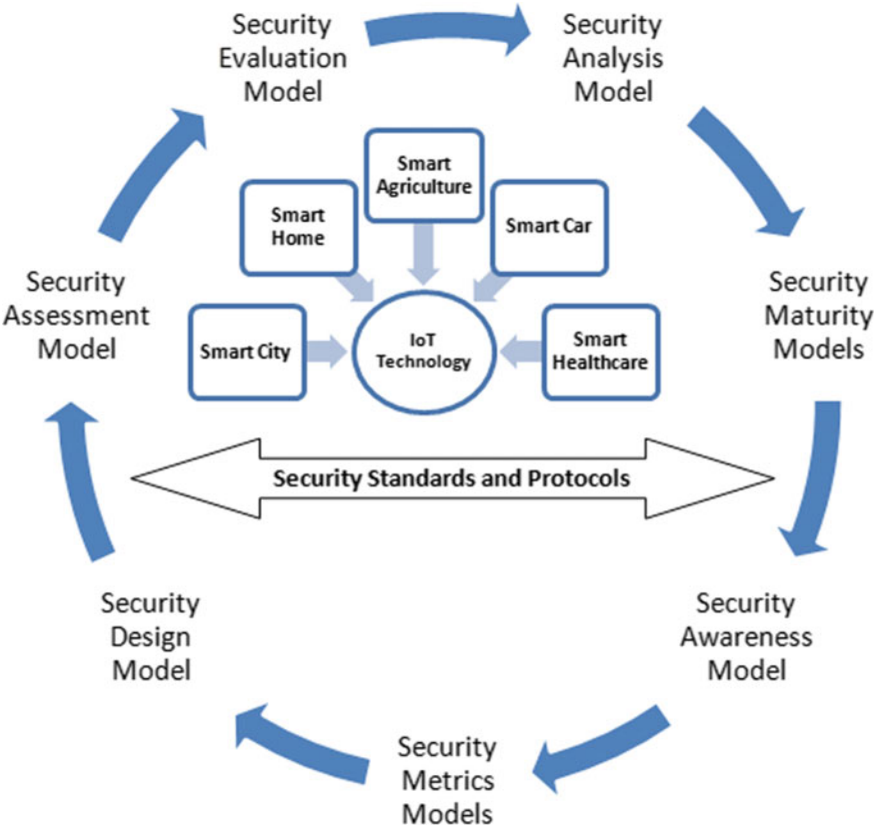

Fig. 1 Comprehensive security mitigation model for IoT-enabled systems

In Fig. 1, a conceptual model for security mitigation for IoT-enabled systems is proposed which if implemented may provide comprehensive security cover to the smart system equipped with IoT technology. Description of the individual components and implementation mechanism of the proposed model are beyond the scope of this paper and may be covered in the subsequent research paper in the future.

4 Conclusion and Future Work

Implementing security to the IoT-enabled smart systems is a matter of concern and although very less data exist which showcase the exploitation of such systems but it does not provide guarantee that such smart systems may not be exploited in the near future. Furthermore, if the harm caused is limited to financial aspect then we may get over it by time but if the harm is done to people involved then it is unacceptable.

In the study, we have seen that the basic stakeholder and consumer of such smart system are people and then are the only ones who may be target in the future for malicious intents. So safeguarding the IoT-enabled smart systems is a must and should be practice from the very beginning when such systems are conceptualized and realized.

The future work may include providing description of the individual components of the proposed model. Another future work may include providing implementation mechanism. One more promising future work may include implementing the proposed model on some newly developed IoT-enabled systems and assess its impact when it is practically put to use.

References

1. Atzori, L., Iera, A., Morabito, G.: Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. Ad Hoc Netw. **56**, 122–140 (2017)
2. Patel, K.K., Patel, S.M.: Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. Int. J. Eng. Sci. Comput. **6**(5) (2016)
3. Sadeghi, A.R., Wachsmann, C., Waidner, M.: Security and privacy challenges in industrial internet of things. In: Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE, pp. 1–6 (2015, June). IEEE
4. Li, S., Tryfonas, T., Li, H.: The Internet of Things: a security point of view. Internet Res. **26**(2), 337–359 (2016)
5. Banerjee, C., Banerjee, A., Murarka, P.D.: Measuring software security using MACOQR (misuse and abuse case oriented quality requirement) metrics: defensive perspective. Int. J. Comput. Appl. **93**(18) (2014)
6. Banerjee, C., Banerjee, A., Murarka, P.D.: Measuring software security using MACOQR (misuse and abuse case oriented quality requirement) metrics: attackers perspective. Int. J. Emerg. Trends Technol. Comput. Sci. **3**(2), 245–250 (2014)
7. Hossain, M.M., Fotouhi, M., Hasan, R.: Towards an analysis of security issues, challenges, and open problems in the internet of things. In: 2015 IEEE World Congress on Services (SERVICES), pp. 21–28 (2015, June). IEEE
8. Banerjee, C., Pandey, S.K.: Software security rules, SDLC perspective. arXiv preprint arXiv: 0911.0494 (2009)
9. Banerjee, C., Banerjee, A.: IMPETUS an Interdisciplinary Research Journal **2**(1). St. Xavier's Jaipur (2014)
10. Banerjee, A.B., Murarka, P.D.: An improvised software security awareness model. Int. J. Inf. Commun. Comput. Technol. **1**(2), 43–48 (2013)
11. Gope, P., Hwang, T.: BSN-care: a secure IoT-based modern healthcare system using body sensor network. IEEE Sens. J. **16**(5), 1368–1376 (2016)
12. Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., Shen, X.S.: Security and privacy in smart city applications: challenges and solutions. IEEE Commun. Mag. **55**(1), 122–129 (2017)
13. Baranwal, T., Pateriya, P.K.: Development of IoT based smart security and monitoring devices for agriculture. In: 2016 6th International Conference Cloud System and Big Data Engineering (Confluence), pp. 597–602 (2016, Jan). IEEE
14. Joo, J.W., Lee, J.K., Park, J.H.: Security considerations for a connected car. JoC **6**(2), 1–9 (2015)