Clinical Cancer Investigation Journal-ISSN: 2278-0513

Vulnerabilities in the Context of the Internet of Things

Abstract

The Internet of Things refers to the objects and equipment in our environment connected to the Internet network and controlled and managed by applications in smart gadgets. Simply put, the Internet of Things refers to the connection of sensors and devices with a network through which they can interact with each other and their users. The present research investigates the mechanism of harm from the Internet of Things. The descriptive-analytical research gathers data from library sources. The fast development and implementation of the Internet of Things-based technologies provide various opportunities for technical progress in various dimensions of life. The main goal of the Internet of Things technologies is to simplify the processes of various types, ensure the better efficacy of the systems (specific technologies or processes) and finally improve life quality. Studies have suggested that security in the Internet of Things is a major concern that should be investigated to meet the goals of the Internet of Things. The Internet of Things architecture is expected to manage billions of related cases. The Internet of Things can be affected by hardware and network threats and smart application threats, which target various communication channels. For this, security and privacy protection issues should be regarded for the Internet of Things, so they are addressed at different scales and contexts.

Keywords: *Internet of Things, Internet architecture, Smart mobile phones, Security software*

Mahdi Pourbaferani[1]
[1] *MSc, Payame Noor University, Tehran, IRAN (*Corresponding Author) mahdi.pourbaferani@gmail.com*
Davood Karimzadgan Moghaddam[2]
[2] *Associate Professor, Department of IT and Computer Engineering, Payame Noor University, Tehran, IRAN*
Davood Vahdat[3]
[3] *Lecturer, Department of IT and Computer Engineering, Payame Noor University, Tehran, IRAN*

Introduction

The Internet of Things (IoT) is a novel concept in the world of Information and Communication Technologies; however, this term was first developed by Kevin Ashton in 1999[1], which described a world in which everything, including inanimate objects, can have a digital identity, thereby allowing computers to organize and manage them. Kevin Ashton proposed that objects (goods and devices) are connected to and exchange data. IoT combines embedded sensors, computing and communication technologies. IoT is aimed at providing integrated services anytime and anywhere. IoT technologies have a pivotal role everywhere and are considered the fourth revolution of modern technologies, following Information Communication Technologies (ICT).

Using IoT, the smart urban structure establishes permanent and real-time communication by connecting electronic devices installed across the urban infrastructure to a cloud space and transferring information to the main server. Here, the main server analyzes and processes the data and transfers the commands to the devices through the cloud space. In this cycle, the main server creates the capability of learning and acquiring experience and improves its functions over time.

One of the major concerns of incorporating IoT into the real world comes from its security aspects. The IoT architecture is supposed to deal with a population of billions of objects interacting with each other, humans and virtual entities. These interactions should be protected, i.e., the information and services provided to all stakeholders and the number of incidents affecting the IoT. However, protecting IoT is a complex task. The number of malicious attacks which arise from global connectivity (access for all) and accessibility (ubiquitous access) as the main IoT processes may be confusing. In sum, the inherent complexity of IoT requires more complicated designs and effective, compatible and scalable security mechanisms.

Almost half of the professions which use IoT fail to determine if their networks are in danger. Since many IoT companies are willing to invest in relevant security issues, one can be hopeful to see this number decline. So far, many IoT vendors have failed to develop internal security software. The major cause of this is the lack of security standards in IoT.

As the applications of this technology development, it is imperative to gain a true picture of security threats in IoT, especially in settings we use this technology. The ever-increasing growth of IoT and the resulting development of communications in this regard have caused a major concern. Privacy violation, cyber-attacks, especially attacks aimed at the infrastructure of foe nations, and terror attacks, among others, are parts of these concerns. On the other hand, vulnerabilities, attacks, safety and security issues, failure to provide appropriate solutions, and the amazing development of IoT signify the importance of this subject.

Theoretical Foundations of the Research

The Internet of Things

The Internet of Things (IoT) refers to billions of devices deployed worldwide, now connected to the Internet, gathering and sharing data. Various definitions of IoT have been offered

[1] **Alessandro Bassi, Martin Bauer, Martin Fiedler**

by different research associations based on their approach to the advantages of this phenomenon. IoT denotes the connection of objects and devices to the Internet. IoT is a network of physical objects or equipment embedded in electronic parts, software, sensors and connections which can provide services or values by exchanging information with the producer, operator and other devices (Bauer et al., 2016). The Gartner Institute defines IoT as a network of physical objects, including aggregate technologies, to interact and communicate with internal and external environments. On the other hand, IDC defines IoT as a network of uniquely identifiable networks of objects which establishes local and global communication without interaction with the man but by using IPs (Esmaeil-Khou, 2016).

Applications of the Internet of Things

Thanks to cheap computer chips and widespread wireless networks, it is possible to connect all objects from a small tablet to a large plane to the Internet and convert them into the IoT context. Connecting objects to the Internet has a wide range of benefits. Today, people have seen and used these benefits in smart mobile phones, laptops, tablets, gadgets, etc. It is thus concluded that mobile phones, laptops, tablets and other gadgets are regarded as useless if they are not capable of connecting to the Internet. The issue of the Internet connection is not only significant for the said devices but is also key for all other "things". IoT has a simple concept essentially and refers to everything in the world connected to the Internet. Thus, almost every physical object, if capable of connecting to the Internet to exchange information in the network without human intervention, or to be controlled through the Internet, can turn into an IoT device.

An incandescent light bulb switched on and off by a smartphone is considered an IoT device. Also, a motion sensor, smart thermostat connected to the Internet at an office, and smart office and passageway lights on the street connected to the Internet are examples of IoT. An IoT device can also range from the cuteness of a child's doll to the complexity of a driverless truck. Some large devices may include many smaller IoT components, such as jet engines, which currently have thousands of sensors that gather data and send them for immediate processing. These operations are performed to ensure the efficacy of the jet engine performance. On a larger scale, one can refer to smart city projects, which are big sources of various sensors that help humans better perceive and control their environment. Examples of IoT are noted in various industries, including auto, entertainment and health care.

Disadvantages of the Internet of Things

Serious security disadvantages also accompany a wide range of IoT-based benefits. Market time and profit-based professions, along with a lack of relevant regulations, have led producers to ignore security considerations and design vulnerable Internet devices, thus allowing the penetration of the enemy who can misuse these devices at low costs or even without any trouble. Negligent security considerations cause the disclosure of sensitive information from an unprotected video streaming of child monitors (M. Stanislav & T. Beardsley) and engender unauthorized voice recording, emails, and password breaches by the Internet-connected toys (Franceschi-Bicchierai, Lorenzo). In addition, poorly-designed devices allow for executing arbitrary commands and re-programming of the operating system of the device (E. Bertino and N. Islam). Considering the deployment of the Internet of Things devices, malicious manipulations can negatively impact the security and flexibility of the whole Internet. One of the major concerns of using and implementing this new technology is its security and privacy. Security must be tightened to avoid the detection of unauthorized access to users. By privacy, it means controlling users' data by themselves rather than by others. Another issue that arises from high dependence on data and IoT -based devices is reliability. By reliability, it is meant that devices must effectively operate to never encounter any problems. In addition to IoT, the data transmitted between the devices and the Internet must be reliable because providing unreliable data is a major concern that may cause unnecessary or mistaken feedback.

Atzori et al. (2010) have discussed two visions of IoT, i.e., things-oriented and Internet-oriented. Programming designers have also investigated research challenges and the most relevant activating technologies by focusing on their roles rather than their technical details. Authors have also discussed the significance of security, stating that widespread limitations such as limited energy and computing capacity of IoT devices hinder the implementation of complicated security mechanisms (L. Atzori, A. Iera, & G. Morabito).

Gubbi et al. (2013) researched the applied areas of IoT and relevant challenges in another project.

Further, Xu et al. (2014) provided an analysis of the main technologies behind the Internet of Things and multi-layer architecture, reviewing industrial applications of IoT. They concluded that due to the specific characteristics of the Internet of Things, such as deployment, mobility and complexity, this paradigm suffers from severe security weaknesses, which is not tolerable in the area of IoT.

Moreover, Al-Fuqaha et al. (2015) reviewed the applied domains of the Internet of Things, revealing the technologies and communication protocols adopted by the Internet of Things. The authors have also differentiated between six categories to provide IoT-based services: detection, measurement, communications, computations, services and semantics.

Security of the Internet of Things

While a certain number of contributions specifically deal with IoT and relevant technologies architecture, a large body of literature concerns its security aspects.

Sicari et al. (2015) analyzed the solutions to the security of the Internet of Things. Because communication technologies and protocols of IoT are different from traditional ICT, their security solutions must also be different. A review of many academic projects reveals that despite numerous efforts in this regard, many research questions remain. Authors have also stressed that there is still a lack of a regular and integrated vision to guarantee the Internet of Things. They also analyzed the international projects in this area and pointed out that such efforts are usually aimed at designing specific IoT programs. Mosenia et al. (2017) used the CISCO's seven-level reference model to provide various scenarios of the corresponding attack.

Vulnerabilities of the Internet of Things

Consistent with specified methodologies, a comprehensive analysis of research projects on the security of IoT reveals nine categories of IoT vulnerabilities as follows:

1. Lack of Physical Security

Most IoT devices independently operate in environments where no labor care is provided (R. Mahmoud, T. Yousuf, F. Alou). With little effort, an intruder may gain unauthorized physical access to such devices and bring them under his control. As a result, the intruder may damage the devices, use the encrypted schemes, duplicate their operating systems by using a malicious node and easily control or corrupt their cyber information (Wurm, 2016).

2. Insufficient Energy

IoT devices have limited energy and lack the technology or mechanism for automatic renewal. An intruder may drain the energy stored by sending illegitimate and corrupted messages, making the devices inaccessible to the users and authentic processes (Trappe, 2015).

3. Insufficient Authentication

Specific limitations within the IoT paradigm, including limited energy and computational power, challenge the execution of complex authentication mechanisms. For this, an intruder may use ineffective authentication approaches to connect fake malicious nodes or breach data integration, thus infiltrating IoT devices and network communications. In this situation, exchanged and used authentication keys are always at risk of being lost and corrupted. As a result, advanced authentication algorithms cannot be sufficient when the keys are not safely stored or transferred (Vidgren, 2013).

4. Inadequate Encryption

Data protection in IoT, especially in critical CPS (e.g., power installations, production factories, building automation, etc.), is pivotal. Encryption is an effective mechanism to store and transmit data in a way that only authorized users can use. Since the capability of encryption systems depends on their designed algorithms, limitations of IoT sources also affect the capability and efficiency of these algorithms. For this, an intruder may bypass established encryption techniques to disclose sensitive information or perform the control operations with limited and practical efforts (E. Ronen and A. Shamir,2016).

5. Unnecessary Open Ports

Various IoT devices unnecessarily open the ports when operating vulnerable systems, allowing intruders to connect and exploit many vulnerabilities (Sachidananda, 2017).

6. Poor Control

Authentic management must protect IoT devices and data against unauthorized access. Consistent with the literature, most IoT devices with cloud management solutions do not provide complicated passwords (Enterprise, 2015). Moreover, when installed, the devices do not ask to change the default user's credentials. Also, most users have higher permissions; thus, the intruder can threaten the data or the whole Internet by infiltrating the device (Siboni,2015).

7. Inappropriate Patch Management Capabilities

Operating systems of IoT and operating systems of the embedded software must be properly patched to continuously minimize the attack vectors and to increase their performance capabilities. Despite this, there is a large number of cases that suggest manufacturers either do not frequently preserve the security patches or lack the automatic patch updating mechanisms. Moreover, the existing updating mechanisms lack integrity guarantees, making them vulnerable to modification and exploitation (Tekeoglu A. and A. S¸. Tosun,, 2016).

8. Poor Programming Methods

Although strong programming techniques and implementation of security components may increase the flexibility of IoT, many researchers have reported a growing number of operating systems released with known vulnerabilities such as backdoors and root users as main points of access and failure to use Secure Sockets Layer (SSL). Thus, an intruder may easily exploit the recognized security weakness to create a buffer overflow, change information and have unauthorized access to the device (Costin, 2014).

9. Inadequate Auditing Mechanisms

Many IoT devices lack complete stages to log in to the system, which may hide the malicious activities against IoT (Yang, 2015).

Research Literature

The research by Tahmasebi Limoni et al. (2019), entitled: "Identification of threats and vulnerabilities in the Internet of Things domain and provision of security guidelines to counter them," concluded that despite the development of various standards in the security and confidentiality of IoT, security issues and relevant perils are not yet to be recognized, requiring such mechanisms as confidentiality, authentication, and access control.

The research by Afshari et al. (2017), entitled: "Categorization of vulnerabilities and challenges of IoT," demonstrated that IoT is made of sensors and actuators and includes various layers of sensors, communication networks, middleware and applications. IoT has various applications in various areas such as housing, smart cities, transportation, business, etc. Because IoT can be used in different situations, its security is also significant.

In the research entitled: "A review of barriers to and ways to prevent IoT challenges", Mirmohammadian et al. (2017) showed that the IoT category in the modern ICT world is a pivotal subject. This technology, they add, entails many advantages, such as reducing time and making things smart. It is also applicable in medicine and agriculture. However, the security aspect of IoT is a challenge that warrants further investigation.

In the research entitled: "Analyzing the application of IoT in a smart city", Valipourian and Eslami (2017) concluded that a smart city requires officials and citizens to use its facilities and achieve positive outcomes. Speaking of positive outcomes of a smart city, one can refer to increasing citizenship welfare, reducing current expenses and saving time and energy, reducing pollution, economic growth, increasing public services and improving the security situation, etc.

Rahmati (2018) did research entitled: "Internet of Things; security and challenges facing it", suggesting the great capacity of IoT has created high expectations of it by converting physical objects of various application areas into Internet hosts. However, intruders may use this great capacity of IoT as a new way to threaten the security and privacy of the users. Therefore, security solutions to IoT should be developed.

Akhundzadeh et al. (2020) did a study entitled: "Security of the virtual space of future smart cities using the fifth Internet generation technologies", concluding that future smart cities which have attracted the attention of scholars can improve life quality. Integrating IoT into models of services to safely manage a city's assets is still a major challenge. The utilization of diverse IoT technologies and several architectural components have caused security threats and emerging vulnerabilities.

The research by Reggio et al. (2020), entitled: "What are the Internet of Things systems in the real-time setting? Views of software engineering experts", found that IoT systems are prevailing, and data analysis suggests that 1. Most IoT systems require human intervention while their advanced learning and self-compliance characteristics are yet to be adopted; 2. Smart industry, smart city, smart buildings and smart houses are, to a large extent, the most relevant area where IoT is applied in and 3. The selection of IoT systems tends to prefer cloud computing to be deployed.

The authors also highlighted that the qualitative characteristics of the IoT systems are reliability, accessibility, functionality, scalability and security.

The research by Kassan et al. (2020) entitled: "A comprehensive review of the Internet of Things: architectures, protocols programs, latest progress, and future guidelines" showed that the emerging concept of IoT is rapidly developing in our modern world where the goal is to improve the quality of life by embedding smart objects, programs and technologies for all-out automation. The number of Internet-connected devices has led to the advent of an IoT revolution. In this context, actuators and sensors are easily incorporated into IoT.

Conclusion

Internet of Things is a prevailing technology that monitors connected smart devices. IoT helps convert many of the fantasies into realities and paves the way for the fourth Industrial Revolution. This technology has an impressive impact on technical, social and economic aspects, human life,

and automation. Scientists claim that the potential benefit of this technology arises when smart objects operate with senses and thinking. IoT is an immense technology that involves various concepts of fog computing, edge computing, communication protocols, electronic devices, sensors, geographical situations, etc. In the near future, the Internet of Things will affect all occupations. IoT transforms the types of devices that are connected to corporate systems. IoT helps businesses gain necessary efficiencies, utilize a wide spectrum of equipment, improve their operations, and increase customer satisfaction.

As the world of communication and information develops, public safety, transportation and health care are improved. As stated, IoT can affect society and business in various respect. IoT has three major benefits affecting the business environment: communication, control and saving costs. IoT can transfer information to people and systems, such as the off or on status of devices, full or empty status of chargers, data from warning systems and sensor data that can control the person's vital signs. In most cases, we previously did not have access to this information which could be gathered rarely or manually. In other cases, an employer or consumer can remotely control a device; for instance, a business owner can switch on and off specific equipment or set them in an environment from a far distance. In the meantime, consumers can use the IoT to open their car locks or switch on the washing machine. The Internet of Things can also send warnings of an anomaly unfolding and provide an automatic response; for example, if a truck brake pad system malfunctions, IoT can send warnings and execute the programming to automatically repair it. This emerging technology which has affected human life, also has many vulnerabilities, which are causes of concern for society.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to the anonymous reviewers and editors for their constructive feedback.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

Afshari, H.; Tajfar, Amir H. & Ghaisari, M. (2017), Classification of IoT Vulnerabilities and Challenges

Al-Fuqaha A., M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.

Atzori L., A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010.

Bauer H, Patel M, Veira J. (2016). The Internet of Things: sizing up the opportunity

Bertino E. and N. Islam, "Botnets and internet of things security," Computer, vol. 50, no. 2, pp. 76–79, 2017.

Costin A., J. Zaddach, A. Francillon, D. Balzarotti, and S. Antipolis, "A large-scale analysis of the security of embedded firmwares." in USENIX Security, 2014, pp. 95–110.

Enterprise H. P., "Internet of things research study," Internet of Things Research Study, 2015.

Franceschi-Bicchierai, Lorenzo, "How this internet of things stuffed animal can be remotely turned into a spy device," https://motherboard.vice.com/en us/article/qkm48b/how-this-internet of- things-teddy-bear-can-be-remotely-turned-into-a-spy-device.

Gubbi J., 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.

eMosenia A. and N. K. Jha, "A comprehensive study of the security of internet-of-things," IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586–602, Oct 2017.

Mir Mohammadian, Seyed M.; Berhelia, S.; Baba Mahmoudi, R. & Akhoundi, Z. (2017), A Review of Challenges and Strategies for Preventing IoT Challenges, 10th Conference on New Research in Science and Technology.

Rahmati, F. (2015), IoT, Security and the Challenges Facing It.

Ronen E. and A. Shamir, "Extended functionality attacks on IoT devices: The case of smart lights," in Security and Privacy (EuroS&P), 2016 IEEE European Symposium on. IEEE, 2016, pp. 3–12.

S. Siboni, A. Shabtai, N. O. Tippenhauer, J. Lee, and Y. Elovici, "Advanced security testbed framework for wearable IoT devices," ACM Transactions on Internet Technology (TOIT), vol. 16, no. 4, p. 26, 2016.

Sachidananda V., S. Siboni, A. Shabtai, J. Toh, S. Bhairav, and Y. Elovici, "Let the cat out of the bag: A holistic approach towards security analysis of the internet of things," in Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security. ACM, 2017, pp. 3 10.

Sicari S., A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in the internet of things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015.

Stanislav M. and T. Beardsley, "Hacking IoT: A case study on baby monitor exposures and vulnerabilities," Rapid 7, 2015.

Tahmasebi Limoni, S.; Ghasemi, Sh. & Ghorbanloo, R. (2019), Identification of common threats and vulnerabilities in the Internet of Things and providing security solutions to counter them.

Tekeoglu A. and A. S¸. Tosun, "A testbed for security and privacy analysis of IoT devices," in Mobile Ad Hoc and Sensor Systems (MASS), 2016 IEEE 13th International Conference on. IEEE, 2016, pp. 343– 348.

Trappe W., R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the internet of things," IEEE Security & Privacy, vol. 13, no. 1, pp. 14–21, 2015.

Vali Pourian, M. & Eslami, H. (2017), Analysis of the use of IoT technology in the smart city, World Congress of Intelligent Technologies 2018.

Vidgren N., K. Haataja, J. L. Patino-Andres, J. J. Ramirez-Sanchis, and P. Toivanen, "Security threats in zigbee-enabled systems: vulnerability evaluation, practical experiments, countermeasures, and lessons learned," in System Sciences (HICSS), 2013 46th Hawaii International Conference on. IEEE, 2013, pp. 5132–5138.

Wurm J., K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial IoT devices," in Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific. IEEE, 2016, pp. 519–524.

L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233–2243, 2014. Yang K., D. Forte, and M. M. Tehranipoor, "Protecting endpoint devices in IoT supply chain," in Computer-Aided Design

(ICCAD), 2015 IEEE/ACM International Conference on. IEEE, 2015, pp. 351–356.

Alessandro Bassi, Martin Bauer, Martin Fiedler, Thorsten Kramp, Rob Kranenburg, Sebastian Lange, Stefan Meissner (2013), Enabling Things to Talk https://link.springer.com/book/10.1007/978-3-642-40403-0

Mirmohammadian.M,Berehlia.S,Babamahmoudi.R,Akhondi.Z (2017),A Review Of Challenges and Solutions to Preventing IOT Challenges

Valipouryan.M, Eslami.H,(2018), https://civilica.com/doc/800907

G.Reggio,M.Leotta,M.Cerioli,R.Spalazzese,F.Alkhabbas,(2020), What are IoT systems for real? An experts' survey on software engineering aspects