Research Journal of Engineering Sciences ISSN 2278 – 9472
Vol. **11(2),** 30-32, May **(2022)** *Res. J. Engineering Sci.*

Short Review

IoT: Major challenges, threats and concerns

Manpreet Sando[*] and Tanuja Kashyap
Department of Electronics and Telecommunication Engineering, Bhilai Institute of Technology, Bhilai House, Durg 491001, India
manpreetsando@gmail.com

Available online at: www.isca.in, www.isca.me
Received 3rd September 2021, revised 20th April 2022, accepted 20th May 2022

Abstract

With various benefits offered, Internet of Things (IoT) is surely going to be one of the widely used technologies to transform lives with its social, economic and technical significance. Major tech giants are already working on it as their core business focus. All in all, it is seen a powerful way that can change the very essence of our living, for the better. But, with great expectations and potential, we absolutely cannot overlook the challenges, concerns and threats, this technology brings with itself. In lieu of providing us with customised suggestions and services, it would leave us susceptible to security concerns like identification and profiling, localisation, as an outcome of blurred public-private borderline, life attacks due to owner identification and tracking. Instead of total automation of these devices leading to mechanical decision making and possible loss of control, a human-machine approach would go a longer way. This paper highlights the current concerns to develop reliable, secure and energy-efficient IoT systems.

Keywords: Internet of things (IoT), challenges to IoT, threats and concerns, ethics in IOT system, Integration with Blockchain and AI.

Introduction

The hot topic among students, researchers and industry people, IoT, acronym for Internet of Things was actually used by Kevin Ashton in 1999 to grab the attention of the executives during a board meeting, is finally getting all the attention it deserves.

IoT allows all devices with an on-off switch or a sensor, to be connected to the internet and other devices. Since it is connected to the internet, it is a giant network of connected devices/things and people to share the collected data, create applications and provide services to improve the quality of life. It allows things and people to be connected barring restrictions of geographical location, time or usage of a different network, path or service. A lot of definitions have been suggested, but all zero-in on the fact, that is it created to build a better world for humans to live and function[1].

Offering benefits of sensing, processing, communicating and actuating without bulky physical databases is having a great impact in making it widely used technology for environmental monitoring, automation and industry 4.0, smart cities, healthcare, intelligent homes, smart farming, factory etc[2].

Discussion

IoT Application Requirements and Challenges: Complicated and complex: because of the involvement of billions of devices, IoT is bound to be complicated and complex to deal with. Integration with AI to give results would be a tedious task because of the integration and coordination with complex systems, keeping in mind memory, processing power, delay constraints in real time systems[3].

Heterogeneity: to realise connecting devices/objects with varied operating systems, platforms and services through IoT to improve the quality of life is one of the major challenges faced. To be future proof we would require services working with multiple IoT applications integrated with AI to give desired outcome[4].

Security and privacy: safe to declare this as one the biggest concern. Since sensitive information is connected to provide the most accurate results, it also puts us at the risk of privacy and security threats. Information like habits, financial details will be freely available and hence it would need frequent updates on the security[5].

Accuracy and speed: with the huge amount of data that is generated by IoT devices, keeping up with it to analyse, and interpret the data would show its real time credibility.

Block chain: keeping innovations in mind, the current centralised client server model would not be able to take care of the need of the future. The contemporary models require connection and authentication through server to maintain a centralised approach. In order to decentralise path, block chain is a popular and viable option. As it is distributed database listing the transaction history among the participating parties of the network, apart from the obvious future prospect handling capacity, it would also be immensely helpful to commute,

process and store the track of transaction happening between billions of IoT devices forming the IoT network without incurring huge amounts to set up data centres[6].

Threats and security concerns: With the internet getting even more control over our lives and its possible exploitation of vulnerabilities by unsuspecting individuals in the vicinity of devices, even when operating at the comfort of our homes or our so called trusted or secured network due to IoT, presents us with newer challenges that we didn't even knew existed a few years ago[7]. Due to less intrusive, more passive and pervasive data collection process in IoT context, the users are less aware of being tracked and monitored and their sensitive information being available online, which in worst case can prove to a threat to their life.

Identification: With more and more data being collected for personalised feel, the threat of identification, i.e., connecting to an Identifier that has access to their personal information and their environment would raise identity theft threat manifolds.

Localization and Tracking: The specifying and recording of a person's internet traffic, GPS data or cell phone location exaggerate security problem by accessing the interaction with nearby located IoT devices by collecting their identity, geographical location and activity, it is almost like digital stalking of individuals[8].

Profiling: Collection and processing data over long periods of time about a person's individual activities and actions for the purpose of classification according to some particular feature is illustrated as the act of profiling. This information is collected secretly and is regularly updated to create a well-built profile. Commonly found instances are personalised ads, music track and video recommendations etc, these are some of the examples of the bigger domain for which it is done can be viewed as targeted advertising by e-commerce industry, credit scoring etc[9].

Life-cycle Transitions: Though not a very commonly occurring problem for most people as the products containing their private information like laptops, smartphones, cameras etc are not shared, but in cases of transition i.e., any kind of lending, giving, interchanging can reveal information stored in them causing major problems.

Inventory Attack: This is another way of illegitimately collecting information about characteristics and features of devices. With the accessibility and addressability of smart devices over internet, providing unauthorized sources the chance to exploit the data paving way for a possible profiling attack disclosing private information about user[10].

Linkage: Integrating various data sources often leads to disclosure of information as the optimization of information from heterogeneous sources is a complex task and often is seen as interchanges or incomplete information when the different authorizations are put together[11].

Ethical issues and legal aspects: IoT technology is seen around us in the form of smart wearable healthcare devices, smart city projects, smart buildings, smart transports, smart environmental monitoring devices. To make these acceptable, we will have to work on the ethics and find solutions to related problems.

So, what exactly is ethics in IoT context and why is it important?

Ethics and Morals are the standard of social behaviour in IoT field. These help us determine what kind of the behaviour is acceptable, and what is not acceptable from IoT devices[12].

Major work needs to be done in the application of ethics in IoT system. Solutions may be implemented single-handedly or collaboratively depending on the need and extent. Some of the ethical issues are discussed below:

Owner identification: we need to clearly define what extent of information is collected. Since these are used for our own benefit, users should be aware of what, how, where and when their information is collected and its exact application.

Public and private borderline: the interconnection of all the devices allows IoT sensors to collect data, without identifying their nature or source i.e., whether it is public data or personal data, would require strong and clearly defined boundaries to ensure that any kind of private information is not freely available over the net.

Life attacks-with the concept of smart cities and smart homes taking over, any kind of security loophole could result in device-hijacking proving serious life threat as our whole environment would be at risk due to interconnectivity of devices. The attacker even if he manages to attack a single device, our whole environment could be in danger because of the presence of multiple weak points[13].

Legal Aspects: Since the boundary between physical and virtual environment is almost transparent in IoT, are we ready for smart environment and technology?– A quick look at the ability of existing laws to protect users.

Internet shutdown is happening a little too frequently these days, than it should. Considering such a case, who will be held responsible for shutdown in medical applications - global internet service provider or the medical service provider? If a service provider is no longer in business, what will be the future of users and what about the handling/sharing/usage of previously collected data? If a small mistake in data collection by these devices leads to faulty diagnosis, leading to loss of life, who will be held responsible? How much data is too much data? What is the limit to which data is collected, is there a time period and pattern in data collection or it is randomly collected data, how do we know what unnecessary data is being collected? How to know if the IoT device is fully secured and not tampered with?

Or simply, in case of an unexpected unexplained shutdown/ failure/malfunctioning, who will be held responsible?[14]

It's time that legal relationships are addressed carefully and in in-depth manner as the IoT system would be integrating multiple partner collaborative ventures and new models of business; classification as will liability, security, privacy, IP, insurance and other regulatory issues would be important for legal relationships and challenges.

Currently, IoT devices are used in combination with artificial intelligence and block chain technology for smart functioning of devices. The future however is not about the concept of "machine intelligence" but "human + machine" essence which can be realised by augmented intelligence. It enhances human intelligence instead of replacing humans to take care using machine learning, data analytics, natural language processing etc. Jobs involving no human involvement can be easily automated by collaborating the sensing and data recording capabilities of IoT and using the AI tools to execute routine tasks with greater efficiency; but the ones dealing with humans, need to be handled carefully. We must never lose control over the systems dealing with humans, by keeping a check on the control and mechanical decision-making of devices and the extent of application of IoT technology.

Conclusion

Despite the innate perks offered in all fields, to achieve global acceptance of its services as a widely used technology, IoT devices would need to work on their security, privacy and legal aspects. We require strong guidelines, laws and policy on online privacy and right to information to address questions like who can control and access information about you and how it is used. Here it was an attempt to bring to light the various challenges, concerns and limitations of this emerging technology. Most of these concerns and threats deal with the safety and privacy aspect which seems to be the underlying concern for all the points discussed. We need to strengthen the IoT system to provide more security and reliability. With various papers already present on this topic, an attempt was made to provide the information in a concise and more user-friendly language for even the layman to understand.

References

1. Atlam, H. F., & Wills, G. B. (2020). IoT security, privacy, safety and ethics. Digital twin technologies and smart cities, Springer Cham, pp. 123-149, ISBN: 978-3-030-18731-6

2. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, 17(4), 2347-2376.

3. Atlam, H. F., Alenezi, A., Alharthi, A., Walters, R. J., & Wills, G. B. (2017). Integration of cloud computing with internet of things: challenges and open issues. IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). pp. 670-675.

4. Xu, K., Qu, Y. & Yang, K. (2016). A tutorial on the internet of things: from a heterogeneous network integration perspective. *IEEE network*, 30(2), 102-108.

5. Atlam, H. F., Alenezi, A., Walters, R. J., & Wills, G. B. (2017). An Overview of Risk Estimation Techniques in Risk-based Access Control for the Internet of Things. Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS). pp 255–260.

6. Atlam, H. F., Alenezi, A., Alassafi, M. O., & Wills, G. B. (2018). Blockchain with Internet of things: Benefits, challenges, and future directions. *International Journal of Intelligent Systems & Applications*, 10(6), 40-48.

7. Nawir, M., Amir, A., Yaakob, N., & Lynn, O. B. (2016). Internet of Things (IoT): Taxonomy of security attacks. Proceedings of 3rd International Conference on Electronic Design (ICED), 321-326.

8. Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks*, 7(12), 2728-2742.

9. Toch, E., Wang, Y., & Cranor, L. F. (2012). Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems. *User Modeling and User-Adapted Interaction*, 22(1), 203-220.

10. Aleisa, N., & Renaud, K. (2016). Privacy of the Internet of Things: a systematic literature review (extended discussion). arXiv preprint 1611.03340. Proceedings of Hawaii International Conference on System Sciences (HICSS-50), 5947-5956.

11. Toch, E., Wang, Y. & Cranor, L. F. (2012). Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems. *User Modeling and User-Adapted Interaction*, 22(1), 203-220.

12. Carron, X., Bosuo, R., Maynard, S. B. & Ahmad, A. (2016). The Internet of Things and Its Impact on Individual Privacy: An Australian Privacy Principle Perspective. *Computer Law & Security Review*, 21(1), 4-15.

13. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things journal*, 1(1), 22-32.

14. Abo Bakr, Ahmed and Azer, Marianne A. (2017). Proceedings of the IEEE 12th International Conference on Computer Engineering and Systems (ICCES). pp 233–237.