Critical Aspects Pertaining to Privacy Preservation of IoT Architecture

M. Sarrab and F. Alshohoumi

Communication and Information Research Center,
Sultan Qaboos University, Muscat, Oman
e-mail: {sarrab@squ.edu.om;alshohoumi}@squ.edu.om

Abstract

With the fast developments of smart devices and the use of Internet of Things technologies, a huge amount of collected and shared data, having significant impacts on several services and applications. However, users are unwilling to disseminate personal private data as it may contain sensitive information. The more private and sensitive the information such as personally identifiable information, credit card information, or personal medical information being shared or disseminated, the more necessary and important to preserve the privacy the that sensitive information. This paper mainly focuses on the privacy preservation of IoT architecture. Starting by discussing privacy in the internet of things. Then analysis of IoT existing architectures, frameworks and standards. Finally, the paper discussed privacy consideration in the current different IoT architectures. Our findings showed that there is a huge demand to devote research efforts to develop new IoT architecture with privacy protection consideration. This effort is part of a funded research project that investigates the internet of things (IoT) security and privacy issues related to architecture, connectivity and collected data.

Keywords

Internet of Things, IoT, Privacy, Privacy Preservation, IoT architectures.

1 Introduction

Internet of things (IoT) includes both physical and virtual things to attain its intended goal. Physical things such as mobile phone and smart connected things can be used to collect data from the surrounding environment (Attie and Meyer-Waarden, 2019). Virtual things such as communication media including Bluetooth, WI-FI, etc. can send collected data to other things. Artificial intelligence and machine learning algorithms can analyze the collected data and send it to other things to interact with them. IoT can be illustrated as networks of networks that includes smart objects, mobile applications, and collected data. To achieve abundant solutions such as improving users targets and enhancing better quality of life (Attie and Meyer-Waarden, 2019). In IoT people and physical objects have the ability to communicate virtually through communication technologies. To exchange knowledge and thus helps in improving life quality (Bujari et al. 2018). Indeed, communication among things and people allows for exchanging and sharing the collected data (Palazzi et al. 2014). That can be used to producing intelligent services. Many technologies (e.g., fog computing, big data, cloud computing, sensing technologies, distributed computing, nanotechnology, wireless communications, artificial intelligence, machine learning, data mining, etc.) support and intervene with IoT to facilitate its development (Islam

et al. 2015). IoT invades our daily life in all fields and provides great benefits. At home, IoT can bring great benefits such as home security, energy efficiency, and comfort (Tan, 2010). For instance, homeowners can use mobile phone to control home smart electronics (WI-FI based) (e.g., smart air conditioning, smart coffee machine, smart light, etc.) from anywhere.

Moreover, IoT helps in increasing home security using Wi-Fi connected CCTV, sensors, and alarms. ioT can be used to provide efficient energy management by using Wi-Fi outlets to turn off unused home electronics (Bujari et al. 2018). The useful application of IoT are those who target the improvement of life quality. For example, it's well-known that the health of population especially in the developed and the developing countries is affected by air pollution that causes dangerous diseases. The IoT is used for measure air pollution by monitoring air quality through detecting the most harmful and risky gases in the air (e.g., CO2, smoke, alcohol, benzene, and NH3) and measuring their amounts accurately. Through IoT, air pollution can be monitored anywhere using mobile or computer. Another useful application of IoT is in Health sector. Healthcare is a very attractive environment for IoT (Islam et al. 2015) and its value in the market is expected to reach 1.1$ to 2.5$ trillion by 2025. IoT in healthcare can be detected in useful use-cases such as aiding rehabilitation, helping management of chronic conditions, tracking and managing changes in people with degenerative conditions, and monitoring critical health for the delivery of emergency healthcare (Bujari et al. 2018). Notwithstanding the great benefits and solutions offered by IoT, its development is surrounded by many challenges and concerns that can affect its sustainability and acceptance among consumers. The major challenges are related to the hardware, interoperability, security, performance, scalability, etc. as discussed in many surveys such as in (Mattern and Floerkemeier, 2010; Chen, 2017; tojkoska and Trivodaliev, 2017). Yet, security and privacy are the most major concerns of IoT that scholars are paying more attention to. The key contribution of this paper is to investigate how privacy is preserved in existing IoT architecture. As privacy, concerns affect the user acceptance of IoT technology. Thus, this research was conducted to analyze the privacy preservation in IoT

2 Privacy in Internet of Things

Internet of things is inspired by calm technology in which it requires no human intervention. IoT devices can communicate with other devices automatically via various communication standards (Solangi, 2018). The essence of IoT is to collect data from the surrounding environment using various sensors and transmit collected data via communication standards to the internet. The transmitted data are subject to processing and analysis to be utilized by end users or beneficiaries. This nature of data collection, transmission, and optimization leads to serious privacy concerns. In particular, IoT devices that collect data can incidentally reveal sensitive data. Moreover, the collected data can be sent to untrusted local network or untrusted third party with no users control (Chen et al. 2018). The existing privacy policies of IoT products are perplexing, partial, and misleading because vendors fail to notify consumers (Solangi, 2018). Some consumers think to be anonymous and trust all sensors used for identification and surveillance in public places (Solangi, 2018). Indeed, IoT users believe that they owned the data produced by IoT devices. They do

not have a clear knowledge of how the collected data is used by cloud services or which data it may reveal (Chen et al. 2018). IoT devices can leak sensitive information as shown by recent studies (Chen et al. 2018; Chen et al. 2015; Barker et al. 2014). Researchers showed that the current smart sensors can be used to collect data about user's mood, stress level, demographics info, smoking habits, sleep patterns, happiness, level of exercise, etc. (Solangi, 2018). The collected data can be shared which lead to revealing an individual's private information. For example, the data collected by smart switches, smart thermostats, and smart power meters can leak information such as whether a home is occupied (Chen et al. 2018; Chen et al. 2015). Furthermore, IoT devices such as rooftop solar panels can reveal home location (Barker et al. 2014). In solar energy analytics, the energy data can leak location information, which can cause location-based privacy attacks (Chen et al. 2018). Moreover, individuals suffering from sensitive medical conditions such as seizures may be burdened if their data shared publicly (Solangi, 2018). The large scale of data collection by IoT devices poses significant privacy challenges such as revealing sensitive information related to the user's activities that may impede the development IoT. Revealing sensitive information without individual consent may cause serious problems especially in critical fields such as the military sector and healthcare. For instance, Strava fitness app posts a map of its user's activity on the internet. Security researchers showed that this public activity map imposed a severe threat to U.S national security by indirectly revealing the locations and behaviors or attitudes of U.S military bases and personnel in Syria and Iraq (Chen et al. 2018). The data are the heart of IoT in which IoT devices collects data and send it for processing and analysis via communication channel (Attie and Meyer-Waarden, 2019). Thus, data privacy in IoT must be preserved to keep consumers trust from one side and keep a good reputation of service providers from another side.

3 IoT Architectures, Frameworks and Standards

Through reviewing and tracing the IoT architectures, it was noticed that the earlier architectures which were illustrated in the years 2008 until 2010 did not demonstrate a comprehensive meaning of IoT nature such as IoT architectures in (Tan, 2010). The accepted IoT architecture was proposed in (Wu et al. 2010). Figure 1 presents the three layers of IoT architecture.

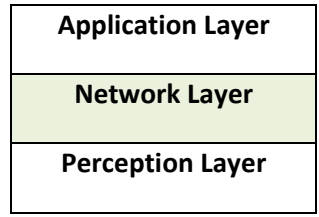

Figure 1: Three Layers IoT Architecture

It simply described that IoT is composed of three layers. The perception layer involves all devices that are used for sensing and collecting data from the surrounding environment such as RFID, 2-D barcode, and even nanotechnologies. The network layer is the core of IoT in which is used for transferring the collected data to the layer

above (the application layer) through communication media such as Wi-Fi, Bluetooth, ZigBee, etc. The top layer is the application layer, which basically is used for managing IoT applications. Nonetheless, it still did not provide a comprehensive meaning of IoT. The later IoT architectures were improving this architecture by solving the challenges encountered by IoT such as huge data collection processing, scalability as Figure 2 presents (Adat and Gupta, 2018; Guo, et al. 2018).

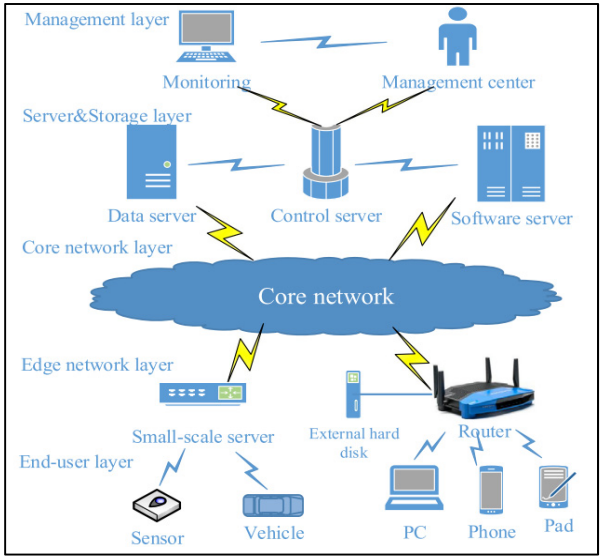

Figure 2: A scalable architecture for IoT based on transparent computing (Guo, et al. 2018).

So far, there is no standard IoT architecture (Abi Sen et al. 2018). The following table presents the current IoT architectures for the purpose of detecting the privacy aspect in these architectures:

Approach	Year	Layers/Components	Remarkable
IoT Five-layer Architectures	2008	Application, Middleware, Internet, Access Gateway and Edge technology layers	The provided architecture did not consider the interoperability issues, as there are no global standards on that year. The designed architecture missed storage and processing layers (Tan, 2010).
IoT Five-layer Architectures with three components in the bottom layer	2010	Application, Middleware, Coordination, Backbone network, edge technology layers	The provided architecture is an extension of the previous architecture that added more details of IoT through adding processing layer. It has more IoT features, such as traffic through the network layer, storage through the coordination layer and packet recognition from different apps (Tan, 2010).

IoT Three-layer Architecture	2010	Application, network and perception Layers	The provided architecture was the accepted three-layer structure of IoT. This architecture helps in understanding the technical structure of IoT at the early stage of development. The designed architecture cannot express all features and connotation of IoT (Wu et al. 2010).
IoT Five-layer Architectures	2010	Business, application, processing, transport, and perception	This architecture is an extension of previous architecture that provided a complete understanding of IoT features and meaning. The designed architecture is more helpful to understand the essence of IoT and it is significant. The designer theoretically describes each layer (Wu et al. 2010).
General Architecture of Trusted Security System Based on IoT	2011	A trusted user module, trusted perception module, trusted network module, trusted terminal module and trusted agent module	The trusted user module includes a trusted user authentication system based on IoT. The general architecture of trusted security system based on IoT is claimed to help to decrease the potential risks of the network that may occur due to access of untrusted users as well as it can enhance security defense (Li et al. 2011).
IoT Architecture Based on Integrated PLC and 3G Communication Networks	2011	Application, network, aggregation and perception layers	This architecture is designed with the consideration of IoT scalability issues by combining two complex communication networks: 3G and PLC. The IoT architecture based on integrated PLC and 3G communication networks were expected to help in the development of the promising technology of IoT (Hsieh and Lai, 2011).
End-to-End two-way authentication security architecture for IoT,	2012	Datagram Transport Layer Security (DTLS), Transport layer, Routing layer and physical and MAC layer	This security architecture is based on public key cryptography technique (RSA) and works on top of standard low power communication stacks. The prescribed architecture elaborates the underlying data and communication flow between a subscriber, gateway, access control server, and internet-enabled certificate authority (Kothmayr et al. 2012).
IoT Five-layer Architectures	2012	Business, application, middleware, network, and perception layers	This architecture has five layers. Perception layer includes business model, flowcharts and graphs; the application layer is as smart applications and management layer. Middleware layer is an information processing layer that considers different components including ubiquitous computing, database, service management, and a

			decision unit, the network layer includes security transmission and 3G, UMIS, Wi-Fi, Bluetooth, Infrared, ZigBee ...etc., perception layer considers physical objects and RFID, Barcode and Infrared sensors (Ray, 2015).
Common Architecture for Integrating the Internet of Things with Cloud Computing	2013	CloudThings service platform(IaaS), CloudThings developer suite(PaaS) and CloudThings operating Portal(SaaS)	The proposed architecture integrated IoT with cloud computing. Actually, the online platform assists system integrators and solution designer to build a complete infrastructure of things application for developing, operating, deploying and combining things applications and services. However, Such integration may pose privacy issues due to storing data in the cloud (Guo, et al. 2018).
Hierarchical security architecture	2013	Application, Middleware, Network, and perceptual layers	This three-layer architecture is designed to protect against inherent openness, heterogeneity, and terminal vulnerability. It's a 2D security architecture in which the vertical division narrows down the complexity of the cross-layer security interaction, and the transverse division based on data flow clears the processing logic of the security mechanism (Zhang and Qu 2013).
Object-based Security Architecture (OSCAR)	2014	Consumers, Could or In-Network Proxy Servers, Authorization Servers, and Producers	This architecture leverages the security concepts both from traditional connection-oriented approaches and content-centric. It supports facilities such as multicast and caching and does not affect the radio duty-cycling operation of constrained objects while providing a mechanism to protect from replay attacks by coupling DTLS scheme with the CoAP (Vučinić et al. 2015).
Four-layers Architecture Service-oriented Architecture of IoT	2015	Sensing, network, service and interface layers	In this architecture, the sensing layer acts as the perception layer which has all devices such as RFID Tag, Intelligent sensors, RFID readers, WSNs and BLE devices as well as the data sensing acquisition protocols. Network layer includes Mobile, social networks, WSNs and WLAN. Service layer includes service division, service integration, and service composition and the interface layer. This architecture provided a solution to the challenge of heterogeneity, interoperability among

			heterogeneous IoT devices with SOA (Li et al. 2015)
IoTNetWar	2015	Application, C4ISR management, gateway communication physical sensing layers.	This architectural framework-IoTNetWar presented the integrity between weapons, military personnel, and overall warfare on the conjugation of sensors, gateways, internet, and cloud-based services (Ray, 2015).
Four-layers Architecture Decentralized Data and Centralized Control IoT architecture	2016	Application, control, network, and device layers	This architecture considers security, SD-Gateway that provides many important functions such as firewall, packet encapsulation, and decapsulation, address translation (NAT), enabling data storage through fog computing, and packet forwarding. Central control will lead to scalability limitation and can impact security enhancement. However, there was a lack of an intelligent algorithm to decide which kind of data must be stored locally in fog nodes, which sort of data has to be transmitted to cloud, and which type of data need to removed (Salman et al. 2016).
Four-layers of secured IoT architecture	2017	Application, support, network, and perception layers	This architecture is claimed that it analyzed security challenges in all IoT layers and security requirements (Yang et al. 2017).
Four-layers IoT architecture	2017	Application, transport, network, and perception layers	This architecture has four layers including perception layer where various devices (Sensors) are used to collect data. This layer is divided into two components: perception node and perception network. This architecture discussed security issues and solutions in each layer (Yang et al. 2017).
Five-layers architecture A scalable and manageable IoT architecture based on transparent computing	2017	Management, server and storage, core network, edge network, and end-user layers	This architecture performance relies on network conditions. Transparent computing in this architecture is useful for improving the scalability of IoT apps by logically splitting the hardware and software of IoT devices. This architecture is effective and efficient as verified experimentally (Guo, et al. 2018).

Table 1: Current IoT Architectures

4 Discussion

As summarized in the Table 2, several IoT architectures were proposed to illustrate the IoT components and provide solutions to the challenges encountered by IoT. It is obvious that the initial IoT architectures started basically with describing the main IoT

components (layers) and didn't consider any challenges as IoT was in its early stage. As the number of IoT devices connected to the internet increased sharply across the years, new challenges emerged and encountered by IoT (e.g., scalability issues, interoperability, security concerns, etc.). To mitigate these challenges, the attention was devoted to improving IoT architecture by suggesting and applying solutions related to scalability, security, etc. However, it is noticeable that there is no consideration of privacy protection in IoT architecture. As discussed in the literature, many privacy concerns are threatening IoT consumers which lead to damage consumer's trust and thus affect the sustainability and the acceptance of IoT among consumers. Therefore, privacy protection needs to be considered and investigated across IoT architecture's layers. This research suggests to investigate data privacy in IoT layers' architecture and to propose data privacy protection technique that help mitigate privacy concerns in IoT.

Year	Approach Aims	Is Privacy Considered?
2008-2010	– Architectures proposed during this period were the initial IoT architecture. They provided the only a description of the basic IoT architecture layers.	– No
2011	– Architectures were proposed to improve scalability issue in IoT as in [18] and considering security as in [17].	– No
2012	– Architecture's focus was on security and providing more details in IoT architecture as in (Khan et al. 2013).	– No
2013	– The target of architectures was to integrate IoT with cloud computing as in, more focus on security (Khan et al. 2013). –	– No
2014	– The architecture was a focus on providing security against reply-attack. –	– No
2015	– The architecture was a focus to solve interoperability among heterogeneous IoT devices through integrating IoT with SOA. –	– No
2016	– The architecture provides SD-Gateway that provides many important functions such as firewall, packet encapsulation, and decapsulation, address translation (NAT), enabling data storage through fog computing, and packet forwarding.	– No
2017	– Architecture targeted scalability issues as in c and discussing security issues as in (Yang et al. 2017). –	– No

Table 2: Discussion of Privacy Consideration in the Current IoT Architectures

5 Conclusion

IoT has undoubtedly changed the world we live in today. Nevertheless, it is considered as a double-sword edge in which it comes up with great solutions to humanity in many critical domains and at the same time threat individuals' privacy. Many privacy violations such as personal information leak, use of the collected personal data by third parties without individual consent, etc., become the major concerns that are encountered by IoT. several IoT architectures were devised to tackle many IoT challenges such as (e.g., scalability issues, interoperability, security concerns, etc.). However, the discussion in the paper revealed that the aspect of pertaining to privacy preservation in IoT architectures was not considered yet. Thus, due to the importance of preserving the privacy to the consumers and IoT providers, there is a crucial need to devote efforts in proposing new IoT architecture with privacy protection consideration.

6 Future Research

Many concerns have threatened IoT consumers' privacy. Protecting data privacy helps in motivating IoT development that is going to change our way in interacting with things. Future research has to focus on improving IoT architecture through considering data privacy protection. There is a need to design a privacy preservation mechanism, which can preserve user's privacy.

7 Acknowledgment

This work was supported by Omental as a part of the project [code: EG/SQU-OT /18/02] under the title of " internet of things (IoT) security and privacy aspects related to architecture, connectivity, and collected data.

8 References

Attié, E. and Meyer-Waarden, L. (2019), "The Acceptance Process of the Internet of Things: How to Improve the Acceptance of the IoT Technology," in Smart Marketing With the Internet of Things, IGI Global, 2019, pp. 21–45.

Bujari, A., Furini, M., Mandreoli, F., Martoglia ,R., Montangero, M. and Ronzani, D. (2018), "Standards, Security and Business Models: Key Challenges for the IoT Scenario," Mob. Networks Appl., Vol. 23, No. 1, pp. 147–154.

Palazzi, C. E., Bujari, A., Marfia, G. and Roccetti, M. (2014), "An overview of opportunistic ad hoc communication in urban scenarios," in 2014 13th annual Mediterranean ad hoc networking workshop (MED-HOC-NET), pp. 146–149.

Islam, S. M. R., Kwak, D., Kabir, M. D. H., Hossain, M. and Kwak, K.-S. (2015), "The internet of things for health care: a comprehensive survey," IEEE Access, Vol. 3, pp. 678–708.

Mattern, F. and Floerkemeier, C. (2010), "From the Internet of Computers to the Internet of Things," in From active data management to event-based systems and more, Springer, pp. 242–259.

Chen, E. T. (2017), "The Internet of Things: Opportunities, Issues, and Challenges," in The Internet of Things in the Modern Business Environment, IGI Global, pp. 167–187.

Stojkoska, B. L. R. and Trivodaliev, K. V. (2017), "A review of the Internet of Things for smart home: Challenges and solutions," J. Clean. Prod., Vol. 140, pp. 1454–1464,.

Solangi, Z. A., Solangi, Y. A., Chandio, S., Aziz, M. B. S. A., Bin HamzahM, S. and Shah, A. (2018), "The future of data privacy and security concerns in the Internet of Things," 2018 IEEE Int. Conf. Innov. Res. Dev. ICIRD 2018, pp. 1–4.

Chen, D., Bovornkeeratiroj, P., Irwin, D. and Shenoy, P. (2018), "Private memoirs of IoT devices: Safeguarding user privacy in the IoT Era," Proc. - IEEE 38th International Conference on Distributed Computing Systems (ICDCS)., pp. 1327–1336.

Chen, D., Kalra, S., Irwin, D., Shenoy, P. and Albrecht, J. (2015), "Preventing occupancy detection from smart meters," IEEE Trans. Smart Grid, Vol. 6, No. 5, pp. 2426–2434,.

Barker, S., Kalra, S., Irwin, D. and Shenoy, P. (2014), "Powerplay: creating virtual power meters through online load tracking," in Proceedings of the 1st ACM Conference on Embedded Systems for Energy-Efficient Buildings, pp. 60–69.

Tan, L. (2010) "Future Internet: The Internet of Things," 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), pp. V5-376-V5-380, 2010.

Wu, M., Lu, T. J., Ling, F. Y., Sun, J. and Du, H. Y. (2010), "Research on the architecture of Internet of Things," 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Vol. 5, pp. 484–487,.

Adat, V. and Gupta, B. B. (2018), "Security in the Internet of Things: issues, challenges, taxonomy, and architecture," Telecommun. Syst., Vol. 67, No. 3, pp. 423–441.

Guo, H., Ren, J., Zhang, D., Zhang, Y. and Hu, J. (2018), "A scalable and manageable IoT architecture based on transparent computing," Journal of Parallel and Distributed Computing, Vol 118, Part 1, pp. 5-13.

Abi Sen, A. A., Eassa, F. A., Jambi, K. and Yamin, M. (2018) "Preserving privacy in the internet of things: a survey," Int. J. Inf. Technol., Vol. 10, No. 2, pp. 189–200,.

Li, X., Xuan, Z. and Wen, L. (2011), "Research on the architecture of trusted security system based on the internet of things," Proc. - 4th International Conference on Intelligent Computation Technology and Automation. ICICTA, Vol. 2, pp. 1172–1175.

Hsieh, H. C. and Lai, C. H. (2011), "Internet of things architecture based on integrated PLC and 3G communication networks," Proc. IEEE 17th International Conference on Parallel and Distributed Systems. - ICPADS, pp. 853–856, 2011.

Kothmayr, T., Schmitt, C., Hu, W., Brünig, M. and Carle, G. (2012), "A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication," in 37th Annual IEEE Conference on Local Computer Networks-Workshops, pp. 956–963.

Khan, R., Khan, S. U., Zaheer, R., and Khan, S. (2012), "Future internet: The internet of things architecture, possible applications and key challenges," Proc. - 10th International Conference on Frontiers of Information Technology, pp. 257–260.

Zhang, W. and Qu, B. (2013), "Security architecture of the Internet of Things oriented to perceptual layer," Int. J. Comput. Consum. Control, Vol. 2, No. 2, pp. 37–45.

Vučinić, M., Tourancheau, B., Rousseau, F., Duda, Damon, A. L. and Guizzetti, R. (2015), "OSCAR: Object security architecture for the Internet of Things," Ad Hoc Networks, Vol. 32, pp. 3–16.

Li, S., Da Xu, L. and Zhao, S. (2015), "The internet of things: a survey," Information Systems Frontiers, Vol. 17, No. 2, pp. 243–259.

Ray, P. P. (2015), "Towards an internet of things based architectural framework for defense," International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), , pp. 411–416.

Salman, O., Elhajj, I., Kayssi, A. and Chehab, A. (2016),"An architecture for the Internet of Things with decentralized data and centralized control," Proc. IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA).

Yang, Y., Wu, L., Yin, G., Li, L. and Zhao, H. (2017), "A Survey on Security and Privacy Issues in Internet-of-Things," IEEE Internet Things Journal, Vol. 4, No. 5, pp. 1250–1258.