IJARCCE

ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 9, September 2021

DOI: 10.17148/IJARCCE.2021.10927

A Survey of Privacy and Security issues in Internet of Things

Shivakumaraswamy GM[1], Praveena K[2], Dr. Ashoka K[3], Dr. Rajanna GS[4]

Assistant Professor, Department of EEE, BIET, Davanagere, India[1]

Research Scholar, Department of ECE, Srinivas University, Mangaluru, India[2]

Associate Professor, Department of CSE, BIET, Davanagere, India[3]

Professor, Department of ECE, College of Engineering & Technology, Srinivas University, Mangaluru, India[4]

Abstract: The Internet of Things paradigm envisions the pervasive interconnection and cooperation of smart things over the current and future Internet infrastructure. The Internet of Things is, thus, the evolution of the Internet to cover the real-world, enabling many new services that will improve people's everyday lives, spawn new businesses and make buildings, cities and transport smarter. Improper device updates, lack of efficient and robust security protocols, user unawareness, and active device monitoring are among the challenges that IoT is facing. Due to the pervasiveness of always connected devices, large amounts of heterogeneous data are continuously being collected. Beyond the benefits that accrue for the users, there are private and sensitive information that is exposed. Therefore, Privacy-Preserving Mechanisms (PPMs) are crucial to protect users' privacy. In this paper, we explore the background of IoT systems and security measures, and identify (a) different security and privacy issues, (b) approaches used to secure the components of IoT-based environments and systems, (c) existing security solutions, and (d) the best privacy models necessary and suitable for different layers of IoT driven applications.

Keywords: IoT, Data security, Data Privacy.

I. INTRODUCTION

The Internet of Things (IoT) refers to a concept of connected objects and devices of all types over the Internet wired or wireless. The popularity of IoT or the Internet of Things has increased rapidly, as these technologies are used for various purposes, including communication, transportation, education, and business development. IoT introduced the hyper connectivity concept, which means organizations and individuals can communicate with each other from remote locations effortlessly. IoT provides the interconnection between multiple heterogeneous devices and sensors that are able to monitor and gather all types of data about machines and human social life [1] The Internet of Things (IoT) foresees the interconnection of billions to trillions [2, 3], of smart things around us uniquely identifiable and addressable everyday things with the ability to collect, store, process and communicate information about themselves and their physical environment [4]. IoT systems will deliver advanced services of a whole new kind based on increasingly fine-grained data acquisition in an environment densely populated with smart things. Examples of such IoT systems are pervasive healthcare, advanced building management systems, smart city services, public surveillance and data acquisition, or participatory sensing applications [5, 6].

The increasingly invisible, dense and pervasive collection, processing and dissemination of data in the midst of people's private lives gives rise to serious privacy concerns. Despite the benefits that can come from collecting data, users are exposing sensitive and private information with possibly untrustworthy entities. These entities can process, analyze and mine data in order to extract useful information, but also sell and/or share the collected data with third parties, using it maliciously. Ignorance of those issues can have undesired consequences, e.g. non-acceptance and failure of new services, damage to reputation, or costly law suits. The public boycott of the Italian retailer Benetton in 2003 [7, 8], the revocation of the Dutch smart metering bill in 2009 [9], or the recent outcry against the EU FP7 research project INDECT [10, 11] are few examples of IoT related projects that experienced huge problems due to unresolved privacy issues. With the growing number of misuse of data and data breaches [12], privacy has been an emergent topic and serious privacy concerns have been aroused. To address these issues, several Privacy-Preserving Mechanisms (PPMs) and tools have been proposed [13, 14, 15].

II. IoT Privacy and Security architecture

The IoT Privacy and Security architecture reference model is depicted in figure-1 which is an updated version of IERC [16]. This architectural model is based on visions of the IoT and can be summarized as: Anyone and anything interconnected anywhere at any time via any network participating in any service. Our reference model describes the entities and information flows of IoT applications.

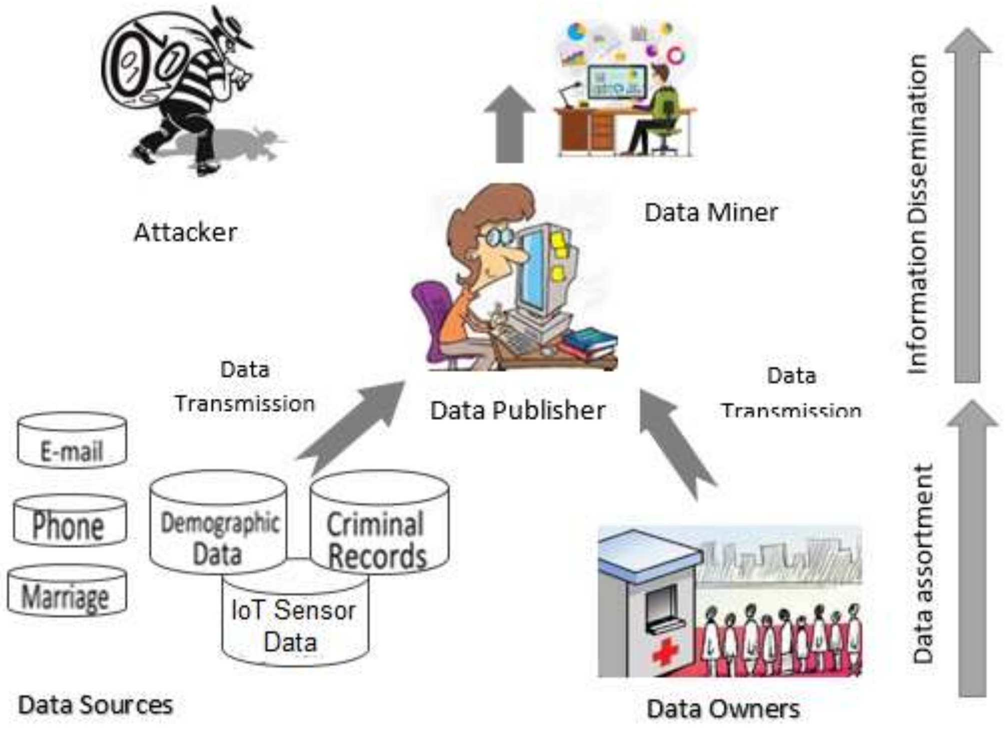

Figure 1. IoT Architectural reference model

Privacy is a very broad and diverse notion for which literature offers many definitions and perspectives [17]. From a historic view, the notion of privacy shifted between media, territorial, communication, and bodily privacy. With the increasing use and efficiency of electronic data processing information privacy has become the predominant issue today. Information privacy was defined by Westin in 1968 as “the right to select what personal information about me is known to which people” [18]. The notion of personal information is necessarily fuzzy, since privacy is a deeply social concept and subject to greatly varying individual perception and requirements [19, 20]. Hence, care must be taken when designing new systems and services to carefully assess the sensitivity of the involved information and relating user requirements, e.g. as businesses are starting to implement in privacy impact analysis’s (PIAs). Ultimately, our definition must be understood such that the user may define what he considers personal information.

III. Literature Review

The authors in [21] stated that there are various challenges, such as jamming and spoofing attacks and other unauthorized access, which have compromised the integrity of the user’s data. There are potential solutions that can help the individual to implement various security measures that can help to secure their IoT devices. According to [22], various privacy threats have emerged in the present time, and they can penetrate IoT Technologies and their integrated network. It is not easy to manage the security of IoT devices in businesses and organizations. The organizations must deploy monitoring and scanning tools for all the IoT devices that could detect any kind of threats related to privacy and try to mitigate the risk of being breached. Traffic interceptors and analyzers help identify and investigate various cyber threats.

There are various studies as well as services that have been conducted on the current trends in IoT security [23]. Multiple services have presented some of the challenges or attack vectors to various IoT devices and their guards.

Various simulation tools, modelers, and the availability of numerous platforms that can confirm this security protocol can also help in producing the protocol related to novel IoT security. It is fair to say that there has been rapid progress in terms of research related to IoT security and various simulation tools as well as modelers have supported this research. If the IoT devices failed, then the issues will be severe.

The authors in [24] believe that, despite the enormous benefits the users are getting from the Internet of Things, there are challenges that come along with it that need to be looked at. Cybersecurity and privacy risks are the primary concerns that have been cited. These two are posing a massive predicament for many business organizations as well as public organizations. Prevalent high-profile cybersecurity attacks have demonstrated the vulnerabilities of IoT technologies. This is simply because the interconnectivity of networks in the Internet of Things brings along accessibility from anonymous and untrusted Internet, requiring novel security solutions. On the other hand, it is important to emphasize the standards and basic principles of the IoT Cyber Security Framework when it comes to implementing the IoT security system. According to [9], one of the most important measures to consider is the termination of a contract consisting of different devices with different communication protocols. The difference in protocols hinder separate service contracts from implementation and are fundamental elements that must be present in the cybersecurity structure of every Internet of Things. He demonstrated that to ensure the reliability of the IoT framework in the cybersecurity arena, some small steps need to be taken to help mitigate the challenges of IoT cybersecurity. In addition, the authors in [25] showed that scalability is also an essential measure of the success of the cybersecurity Internet of Things framework. Analysts said the IoT environment needs to be scalable enough to handle a billion Internet-related and cybersecurity challenges. In addition, the magazine showed that the IoT cybersecurity environment should also support testability, such as integration testing, component testing, system testing, and compliance testing, effectively reducing challenges and risks.

In the same context, the authors in [26] described some of the current IoT cybersecurity solutions. Some basic security measures are implemented by the supplier, and state that it is not profitable for the supplier to produce high-quality solutions. In the case of cybersecurity of the Internet of Things, companies are unlikely to develop the right solution.

Moreover, the authors in [27] describe the currently embedded mobile and cyber-physical systems as ubiquitous, from industrial control systems, modern vehicles to critical infrastructure. Current trends and initiatives, such as Industry 4.0 and the Internet of Things (IoT), promise innovative business models and new user experiences through strong connectivity and the operational use of new generations of embedded devices. These systems generate, process, and exchange large amounts of relevant data. Security and confidential beliefs that make cyber-attacks an attractive target for the Internet of Things system cause physical harm and disrupt people's lives. Cybersecurity and privacy are important because they can pose a threat. The complexity of these systems and the potential impact of cyber-attacks pose new threats to related industrial IoT systems. Possible solutions to security and privacy challenges are general security frameworks for industrial IoT systems. Current IoT systems have not improved enough to secure the desired functions.

Therefore, there has been extreme significance in the study and research of various security issues in IoT. One of the main objectives in terms of IoT security is to provide privacy, confidentiality, and to ensure that every user can get better protection, infrastructures, and a guarantee to the availability of various services offered by the ecosystem of IoT. Therefore, the research in various IoT security is gaining necessary momentum with the help of different simulation tools as well as multiple computational platforms [28].

With the increasing development of IoT technology and pervasive use of social networks and smartphones, Location Based Services (LBS) has become an active area of research. LBS with IoT offers high degree of flexibility and convenience, but user may breach their privacy if the LBS server is distrustful and malicious. The authors in [29] propose location privacy algorithm that first analyze Dummy Location Selection (DLS) algorithm and also developed an attack algorithm for DLS (ADLS) for testing IoT security and privacy. The concept of location-obfuscation, mix-zone with context awareness was used in [30] that assures location privacy in IoT. This proposed algorithm works effectively for IoT networks with certain threshold no of nodes.

Yu et al. [31] consider IoT devices as weak access points to vital infrastructures (e.g., a medical or military facility) and can be misused to leak sensitive data. The authors have made two main observations regarding IoT systems: (1) network-based approaches are less vulnerable than host-based approaches due to inherent limitations and possible unpatched vulnerabilities on IoT devices; (2) traditional static perimeter defenses are unable to secure IoT devices, since these devices are deployed deep inside the network, with their physical and computational context constantly changing. Therefore, resource limitations make it challenging to secure IoT layers individually. Thorough study was performed on IoT devices vulnerable to Heartbleed [32] according to SHODAN [33] and other sources.

The IoT device layer (also known as perception layer) contains all physical resources that collect/control data (sensors and actuators). However, these resources are highly heterogeneous and resource-constrained. Such constraints pose unique challenges on applying privacy preserving techniques. Thus, IoT devices are subject to several attacks discussed in [34] including node capture, fake node, malicious data, denial of service attack (DoS), timing attack, routing threats, replay attack, side channel attack (SCA), and mass node authentication problem. Therefore, several security measures

DOI: 10.17148/IJARCCE.2021.10927

must be considered when designing this layer as follows: (i) Access control and authentication: to prevent user privacy leaks from open and unauthorized access. Juels et al. [35] present a good solution to implement Selective RFID Jamming as an access control scheme on low-cost tags (ii) Data encryption: to secure data exchange and guarantee safe delivery. Wang [36] presents a nonlinear key algorithm based on displaced calculation to provide data encryption. This key algorithm requires low computational power to provide high security and good data transmission rate. (iii) Secure channel using IPSec: the IPSec protocol [37] offers both authentication and encryption. Raza et al. [38] present a 6LoWPAN/IPsec extension to provide security for IoT devices. The authors demonstrate that IPSec outperforms the standard IEEE 802.15.4 link layer security in IoT environments. (iv) Cryptography technology: to offer privacy protection, confidentiality, authenticity and data integrity. Secure communication protocols include digital signatures and hash values are used to ensure data integrity.

IV. Conclusion

IoT devices and applications are playing an essential role in our modern life. We can see IoT devices almost everywhere from our homes, farms, offices, shopping centers, educational institutes, airports, and many other places to provide us with secure and on-demand services.

Finally, most users are still unaware about the privacy risks of sharing data. This calls for mechanisms to raise users' awareness. For instance, people should be educated about the risks and how they can protect their privacy through changes in their behavior. Currently, there are some frameworks to educate users on privacy matters [39] and others to raise users' awareness [40]. It would be interesting to have combined mechanisms to raise awareness but also educate users by helping them in their privacy-related choices.

References

[1]. Z. Yan, P. Zhang, A. V. Vasilakos, A survey on trust management for internet of things, *Journal of Network and Computer Applications* 42 (**2014**) pp. 120-134.J. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

[2]. Evans D. The Internet of Things - How the Next Evolution of the Internet Is Changing Everything. CISCO white paper **2011**.

[3]. David K, Jefferies N. Wireless visions: A look to the future by the fellows of the wwrf. Vehicular Technology Magazine, IEEE dec **2012**; 7(4):26 –36, doi:10.1109/MVT.2012.2218433.

[4]. Mattern F, Floerkemeier C. From active data management to event-based systems and more. Springer-Verlag, **2010**.

[5]. Presser M, Krco Sa. IOT-I: Internet of Things Initiative: Public Deliverables – D2.1: Initial report on IoT applications of strategic interest **2010**.

[6]. Atzori L, Iera A, Morabito G. The Internet of Things: A survey. Computer Networks **2010**; 54(15):2787 – 2805, doi:10.1016/j.comnet.2010.05.010.

[7]. Benetton to Tag 15 Million Items. RFID Journal. http://bit.ly/XXe4Wi [Online. Last accessed: 2012-09-25], **2003**.

[8]. Albrecht K. Boycott Benetton - No RFID tracking chips in clothing! Press Release. http://bit.ly/49yTca [Online. Last accessed: 2012-09-25], Sep **2003**.

[9]. Cuijpers C. No to mandatory smart metering does not equal privacy! Tilburg Institute for Law, Technology, and Society: Webblog **2009**.

[10]. The INDECT Consortium. INDECT project. http://www.indect-project.eu/ [Online. Last accessed: 2012-10-12], **2009**.

[11]. M¨unch V. STOPP INDECT. http://www.stopp-indect.info [Online. Last accessed: 2012-10-12], **2012**.

[12]. J. Clement, Online privacy in the United States - statistics & facts, (July **2020**). URL https://www.statista.com/topics/2476/online-privacy/

[13]. Y. A. A. S. Aldeen, M. Salleh, M. A. Razzaque, A comprehensive review on privacy preserving data mining, SpringerPlus 4 (1) (**2015**) 694.

[14]. A. Shah, R. Gulati, Privacy preserving data mining: Techniques classification and implications - a survey, Int. J. Comput. Appl 137 (12) (**2016**) 40-46.

[15]. R. Mendes, J. P. Vilela, Privacy-preserving data mining: Methods, metrics, and applications, IEEE Access 5 (**2017**) 10562-10582.

[16]. Vermesan O, et al.. Internet of things strategic research roadmap. *Internet of Things: Global Technological and Societal Trends* **2009**.

[17]. Renaud K, G´a andlvez Cruz D. Privacy: Aspects, definitions and a multi-faceted privacy preservation approach. Information Security for South Africa (ISSA), **2010**, 2010; 1 –8, doi:10.1109/ISSA.2010.5588297.

[18]. Westin AF. Privacy and freedom. Washington and Lee Law Review **1968**; 25(1):166.

[19]. Moore B. Privacy: Studies in social and cultural history. M.E. Sharpe, **1984**.

[20]. Solove D. A taxonomy of privacy. University of Pennsylvania Law Review **2006**; 154(3):477.

[21]. Meng, Y.; Zhang, W.; Zhu, H.; Shen, X.S. Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures. IEEE Wirel. Commun. **2018**, 25, 53–59.

[22]. Siby, S.; Maiti, R.R.; Tippenhauer, N.O. Iotscanner: Detecting privacy threats in IoT neighborhoods. In Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, Abu Dhabi United Arab Emirates, 2 April **2017**; pp. 23–30.

[23]. Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. Comput. Netw. **2019**, 148, 283–294.

[24]. Leloglu, E.Areviewof security concerns in Internet of Things. J. Comput. Commun. **2016**, 5, 121–136.

[25]. Liu, X.; Zhao, M.; Li, S.; Zhang, F.; Trappe,W. A security framework for the internet of things in the future internet architecture. *Future Internet* **2017**, 9, 27.

[26]. Ali, S.; Bosche, A.; Ford, F. Cybersecurity Is the Key to Unlocking Demand in the Internet of Things; *Bain and Company: Boston*, MA, USA, **2018**.

[27]. Sadeghi, A.-R.; Wachsmann, C.; Waidner, M. Security and privacy challenges in industrial internet of things. *In Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, San Francisco, CA, USA, 8–12 June **2015**; pp. 1–6.

[28]. Izzat, A.; Chuck, E.; Lo'ai, T. The NICE Cyber Security Framework, Cyber Security Management; *Springer: Basel*, Switzerland, **2020**; ISBN 978-3-030-41987-5.

[29]. Gang Sun, Victor Chang, Muthu Ramachandran, Zhili Sun, Gangmin Li, Hongfang Yu, Dan Liao, Efficient location privacy algorithm for Internet of Things (IoT) services and applications, Journal of Network and Computer Applications, Volume 89, **2017**, Pages 3-13, ISSN:1084-8045, https://doi.org/10.1016/j.jnca.2016.10.011.

[30]. Ismail Butun and Mikael Gidlund, Location Privacy Assured Internet of Things, In Proceedings of the *5th International Conference on Information Systems Security and Privacy (ICISSP* **2019**), pages 623-630 ISBN: 978-989-758-359-9, DOI: 10.5220/0007587906230630

[31]. T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things," in Proceedings of the 14th ACM Workshop on Hot Topics in Networks, HotNets-XIV 2015, USA, November **2015**.

[32]. Z. Durumeric, J. Kasten, D. Adrian et al., "The matter of heartbleed," in Proceedings of the 2014 ACM Internet Measurement Conference, IMC 2014, pp. 475–488, Canada, November **201**4.

[33]. Shodan. March, Devices Vulnerable to Heartbleed [Online]. Available, **2016**.

[34]. K. Zhao and L. Ge, "A survey on the internet of things security," in Proceedings of the 9th International Conference on Computational Intelligence and Security, CIS 2013, pp. 663–667, December **2013**.

[35]. A. Juels, R. L. Rivest, and M. Szydlo, "The blocker tag: Selective blocking of RFID tags for consumer privacy," in Proceedings of the 10th ACM Conference on Computer and Communications Security, CCS 2003, pp. 103–111, USA, October **2003**.

[36]. X. Yi, Y. Liang, E. Huerta-Sanchez et al., "Sequencing of 50 human exomes reveals adaptation to high altitude," Science, vol. 329, no. 5987, pp. 75–78, **2010**.

[37]. S. Kent and K. Seo, "Security Architecture for the Internet Protocol," RFC Editor RFC4301, **2005**.

[38]. S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Things-a comparison of link-layer security and IPsec for 6LoWPAN," Security and Communication Networks, vol. 7, no. 12, pp. 2654–2668, **2014**.

[39]. Hameed SS, Hassan WH, Abdul Latiff L, Ghabban F. **2021**. A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches. *PeerJ Computer Science* 7:e414 https://doi.org/10.7717/peerj-cs.414

[40]. I. C. S. Institute, U. of California-Berkeley, Teaching Privacy, (consulted in September **2020**). URL http://teachingprivacy.org

[41]. A. Boutet, S. Gambs, Inspect what your location history reveals about you: Raising user awareness on privacy threats associated with disclosing his location data, in: Proceedings of the 28th *ACM International Conference on Information and Knowledge Management, CIKM '19,* Association for Computing Machinery, New York, NY, USA, **2019**, p. 2861-2864. doi:10.1145/3357384.3357837.