Personal Data Privacy Challenges of the Fourth Industrial Revolution

Md Mehedi Hassan ONIK*, Chul-Soo KIM*, Jinhong YANG**

*Department of Computer Engineering, Inje University, Gimhae-50834, Korea

** Department of Healthcare and Information Technology, Inje University, Gimhae-50834, Korea

hassan@oasis.inje.ac.kr, charles@inje.ac.kr, jinhong@inje.ac.kr

Abstract— **Fourth industrial revolution (Industry 4.0) promises a connected and smart manufacturing system where internet, machine (physical system) and humans lumped together. Unlike other industrial revolutions, this industrial revolution deals more with information. Device to device (D2D) and Machine to Machine (M2M) communications often generate, preserve and share private information. Personal data has already turned out to be a new commodity and currently identified as a 'new oil' or 'new domain of warfare'. The more information gets generated and accumulated, the more extensive and risky the personal information becomes. Although privacy and security are often bundled together, they are different. This study investigates the privacy attack surfaces of key Industry 4.0 components (i.e. Cyber-Physical System, Artificial Intelligence, additive manufacturing, autonomous vehicle, big data, cloud computing, internet of things, distributed ledger etc). Multi-dimensional privacy challenges, data breaching incidents, regulations and need of a contextual privacy awareness is discussed in this study. Finally, this work elaborates the risk of Personally Identifiable Information (PII) leaking in the era of industry 4.0.**

Keywords— **Fourth Industrial Revolution, Data, Personally Identifiable Information, Industry 4.0, Information Privacy.**

I. Introduction and Background Studies

The concept of this Fourth Industrial Revolution was introduced in the year 2011. German manufacturing industry [1] publicly declared "Industrie 4.0" also known as "fourth industrial revolution", "Industry 4.0". The concept of this Fourth Industrial Revolution was introduced by Schwab [2] in 2016. Industry 4.0 was officially announced in the annual meeting of World Economic Forum in Geneva. Industry 4.0 also known as "industrial Internet" [3], "Integrated Industry" [4] and "Smart Industry" [5]. This revolution is still ongoing and facing multi-dimensional challenges. Several researchers [6], [7] have already mentioned the security side. With legacy security issue this industry will inherit data privacy issues too. So, the privacy of personal data in the era of industry 4.0 requires more investigation.

The divergence of gradual industrial development from year to year was mentioned by Onik [8]. Three vital features to build the skeleton of industry 4.0 are: an autonomous invention by decentralization is to grow smart goods, compatibility brings balance among devices and technologies to increase efficiency. A closer inspection at industry 4.0 expresses high involvement of personal data. However, therefore data privacy is one of the big concern for future industrial revolutions.

Industry 4.0 will expose maximum personal information the world has ever seen. Although people are considering those as an asset, several recent information leaking incidents [9], [10] have shaken the whole world in perspective of data privacy, which motivates us to analyses personal data privacy. About 87% identity of the US citizen is vastly identifiable by 5-digits of their zip code, gender, birthdate only. Korea Internet and Security Agency's (KISA) measured public opinion about data privacy and found major concerns: "undesired and foolish assembly of PII 33.3%", and "illegal use of PII 27.6%". Gemalto's Breach Level Index exposed that on average ten million PII reveal per day where 74% were identity stealing.

To deal with data privacy and security issues, several organizations have initiated laws and regulations to reduce personal data loss [11], [12]. Around 200 billion USD are being exchanged annually to share Personal data. However, those PII or PPII are not always collected illicitly. Sometimes, the user provides their personal data also with appropriate consent.

II. Privacy Attack Surface in Industry 4.0

A. Artificial Intelligence and Robotics

Artificial Intelligence is at the top of this privacy leaking list. Several researchers have identified the privacy risk of AI [13], [14]. Real-time image processing revels human identity and leaks millions of personal information [15], [16]. This study finds the major issues of AI and Robotics in perspective data privacy are:

- No privacy standardization for AI-based technologies
- Consent gathering from the user is inefficient
- AI decision making (profiling) should be monitored

B. Augmented Reality (AR) and Virtual Reality (VR)

To enjoy the world of AR and VR, we must share some personal data. Recent studies [17], [18] found the followings by analysis the AR and VR devices from the following companies: mixed reality, Sony, oculus, play station, daydream, Viron, Next, Samsung's Gear VR, HTC's vive. The study found similarity among themselves with respect to

private information gathering. Almost everyone is using cookies or beacons to gather information.

C. Internet of Things (IoT)

Internet of Things (IoT) data privacy was mentioned by several studies in the different domain of use [19]–[21]. A future global network of "things" bring challenges concerning privacy. We, therefore, outline the main reason for IoT data privacy leaking:

- Default Raw data storage
- Ensure the device
- Energy limitation
- Encryption limitation
- Insufficient standardization organization
- Less information from IoT device producer in perspective of device level data collection and sharing.

D. Cyber-Physical System (CPS)

The fundamental enabler of the industry 4.0 is Cyber-Physical Systems (CPS) where critical quality management a must was mentioned by a study by Aich [22]. Privacy revealing in CPS is typically passive [23]. The study mentioned two ways of privacy leaking in CPS:

- Physical: This kind of privacy attack directly interfere with the physical properties of the system. For example, altering the powers of an implantable healthcare chip.
- Cyber: Computer virus, software and network-based attacks are cyber-attack to CPS. For instance, forging sensor data.

Chattopadhyay [24] mentions threat surfaces as in Figure 1.

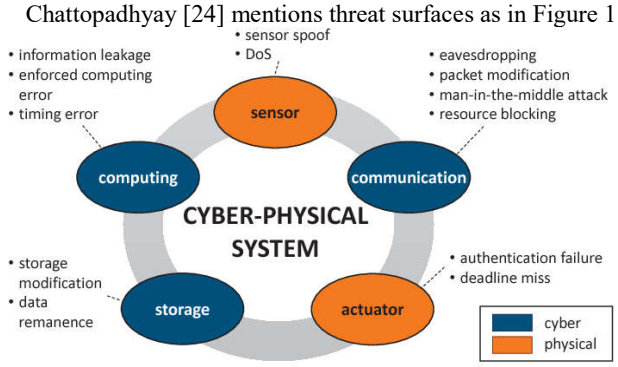

Figure 1. Attack surface of Cyber-Physical System (CPS) [24].

E. Cloud and Big Data

The largest and most critical threat cloud computing poses for organisations today, is the loss of sensitive and personal data and information - both deliberately and inadvertently. [16]. Big Data investigation has become fast, efficient and accurate after the involvement of AI. Key challenges of Cloud and big data are:

- An expert data encryption method
- Physical vulnerability
- Vague data sharing and exchanging policy
- Large-scale data aggregation

F. Blockchain Technology

Blockchain technology versus General Data Protection Regulation (Immutability vs mutability) is key blockchain drawback related to privacy [25]. In one side, blockchain stores data immutably but, personal data must be erasable ethically after use. Storing personal information on a blockchain seriously violate personal data privacy. Identity hiding can be misused, and privacy-breaching may have done unanimously. Moral consideration is overruled in blockchain technology. Blockchain technology in human resource was proposed but the moral thoughts (i.e. privacy) were absent [26].

III. Discussion and Research Challenges

Therefore, this study mentions few of our recommendation and existing solutions:

A. Privacy in Data Processing and Sharing

This is the crucial point to monitor and improve user data privacy. Most of today's Privacy breaching are happening by controller and processer. GDPR complied blockchain system for PII track was presented by a study [25] (Figure 2). Along with financial benefit, the enterprise should consider data privacy too.

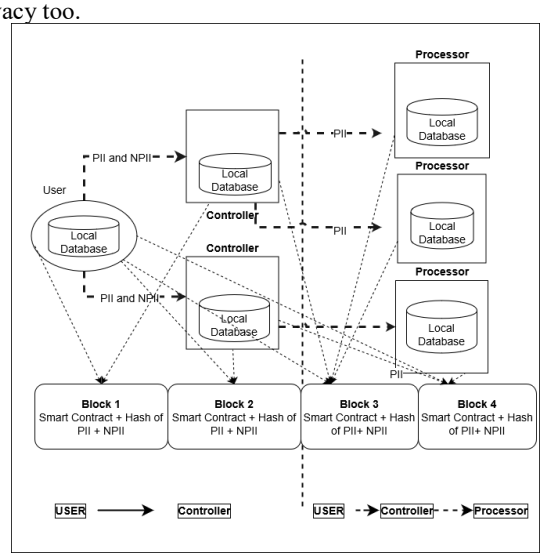

Figure 2. A blockchain based personal data sharing [25].

B. Limitations of Privacy Regulations

Privacy-preserving regulations should be updated according to threat style. GDPR is conflicting to blockchain and imposing strict regulation on data mining which could reduce user experience. HIPAA defined de-identification methods are limited and strict which limiting the research scope in the health care industry. Similarly, Korean regulation does not have enough privilege to inform data branching incidents to users.

C. Privacy by Design (PbD)

A classification of privacy necessities for IoT system was proposed in a study [27] where privacy by design [28], [29]

was at the top of their list. This technique provides privacy from the beginning of system implementation. Privacy by design provides two level security to the system. Firstly, while collecting information from users, the system checks the type of personal data fitness to the context. Secondly, the system can assess the scope of data sharing to the internet and associated risk.

D. Privacy-Preserving Data Aggregation

A novel risk modelling technique was proposed by another study where Risk where collective information clustering at owner side was proposed (Figure 3). That study said android revealed location, unique ID and device storage privacy through collective mobile app permissions [30]. This separate data collection and aggregation at owner side is a key privacy challenges cause, under the fourth industrial most of the companies are developing multi-dimensional service for users.

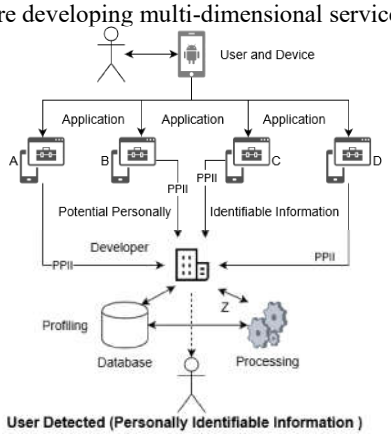

Figure 3. Android devices application privacy permission integration [30].

E. Privacy Awareness

Since privacy was not considered as seriously as security. Therefore, very few researches and implementations were done in this. Trust visualization for object management in the internet of things was discussed by a study [31]. Privacy of Things (PoT), new terminology was introduced by another study [21] (Figure 4). Study stated data flow, receiver, context, risk level should be visible to users for privacy protection.

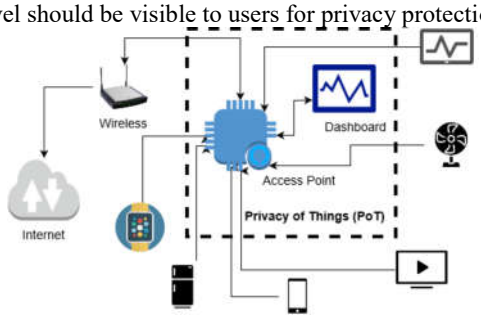

Figure 4. Privacy of Things (PoF), privacy monitirng system for IoT [21].

F. Privacy is not Security

Privacy of our personal information can also be leaked without any technical or security shortcomings. If we look around few recent security breaching incidents [32], often found that the reason for data losses and information leaking didn't happen due to technological disorder rather lack of regulations, monitoring and accountability. Recent data protection regulations like GDPR has been declared as privacy-preserving regulation, not for security [33]. Therefore, several studies have suggested data privacy risk besides data protection measures. Karen [34] suggested instead of creating information security, institutional individuals should focus on data privacy regulations. Personal data breaching costing us tons of money was mentioned by several studies [35]. Therefore, this study now identifies each scope of personal data breaching in almost every technology related to the industry 4.0. Applying security actions are surely effective, however, cannot be a precise way to protect privacy problems.

IV. CONCLUSIONS

The only way of securing personal information is to differentiate security and privacy. As shown below:

$$\text{security} \neq \text{privacy}$$

Till now, technologies that are building the fourth industrial revolution are secured enough to the enduring upcoming threat. However, existing policy, regulations, awareness is still at the infant stage as well as unable to protect personal information vigorously. Obviously, the future industrial revolution must have concreated standardization organization for privacy preserving.

However, this personal information of Industry 4.0 will bring an ethical war in between "data analysis" and "data privacy". On one side, the industrial revolution demands higher data gathering and improved the user experience. Another side, privacy of personal information can never be diminished. We discussed existing technologies and found that privacy by design and context-aware data de-identification is must to improve personal data privacy.

ACKNOWLEDGMENT

This research was funded by Institute for Information & communications Technology Promotion (IITP) grant subsidized by the Korea government (Ministry of Science and ICT) (Grant No. 2018-0-00261) GDPR Compliant Personally Identifiable Information Management Technology for Interent of Things Environment.

REFERENCES

[1] H. Kagermann, W.-D. Lukas, and W. Wahlster, "Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution," *VDI nachrichten*, vol. 13, no. 11, 2011.

[2] K. Schwab, R. Drath, A. Horch, P. Prisecaru, and S. Dais, "Industrie 4.0–Anstoß, Vision, Vorgehen," *IEEE Ind. Electron. Mag.*, vol. 8, no. 1, p. 66, 2017.

[3] S. Bungart, "Industrial Internet versus Industrie 4.0. Produktion–Technik und Wirtschaft für die deutsche Industrie." 2014.

[4] T. Bauernhansl, M. Ten Hompel, and B. Vogel-Heuser, *Industrie 4.0 in produktion, automatisierung und logistik: anwendung, technologien und migration*. Springer, 2014.

[5] S. Dais, "Industrie 4.0–Anstoß, Vision, Vorgehen," in *Handbuch Industrie 4.0 Bd. 4*, Springer, 2017, pp. 261–277.

[6] S. Ryu, Y.-J. Kang, and H. Lee, "A study on detection of anomaly behavior in automation industry," in *Advanced Communication Technology (ICACT), 2018 20th International Conference on*, 2018, pp. 377–380.

[7] S. R. Chhetri, N. Rashid, S. Faezi, and M. A. Al Faruque, "Security trends and advances in manufacturing systems in the era of industry 4.0," in *Computer-Aided Design (ICCAD), 2017 IEEE/ACM International Conference on*, 2017, pp. 1039–1046.

[8] M. M. H. Onik and M. Ahmed, "Blockchain in the Era of Industry 4.0," in *Data Analytics*, CRC Press, 2018, pp. 259–298.

[9] F. Pigni, M. Bartosiak, G. Piccoli, and B. Ives, "Targeting Target with a 100 million dollar data breach," *J. Inf. Technol. Teach. Cases*, vol. 8, no. 1, pp. 9–23, 2018.

[10] P. Kang, "Determinants of Personal Information Protection Activities in South Korea," 2018.

[11] P. Carey, *Data protection: a practical guide to UK and EU law*. Oxford University Press, Inc., 2018.

[12] D. Gozman and L. Willcocks, "The emerging Cloud Dilemma: Balancing innovation with cross-border privacy and outsourcing regulations," *J. Bus. Res.*, 2018.

[13] I. Priyadarshini, "Cyber Security Risks in Robotics," in *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*, IGI Global, 2018, pp. 1235–1250.

[14] K. Siau and W. Wang, "Building Trust in Artificial Intelligence, Machine Learning, and Robotics," *Cut. Bus. Technol. J.*, vol. 31, no. 2, pp. 47–53, 2018.

[15] Z. Qin, J. Weng, Y. Cui, and K. Ren, "Privacy-Preserving Image Processing in the Cloud," *IEEE Cloud Comput.*, vol. 5, no. 2, pp. 48–57, 2018.

[16] Z. Xia, Y. Zhu, X. Sun, Z. Qin, and K. Ren, "Towards privacy-preserving content-based image retrieval in cloud computing," *IEEE Trans. Cloud Comput.*, vol. 6, no. 1, pp. 276–286, 2018.

[17] P. A. Rauschnabel, J. He, and Y. K. Ro, "Antecedents to the adoption of augmented reality smart glasses: A closer look at privacy risks," *J. Bus. Res.*, vol. 92, pp. 374–384, 2018.

[18] J. Ren, M. Lindorfer, D. J. Dubois, A. Rao, D. Choffnes, and N. Vallina-Rodriguez, "Bug Fixes, Improvements, ... and Privacy Leaks A Longitudinal Study of PII Leaks Across Android App Versions," *NDSS 2018 (Network Distrib. Syst. Secur. Symp.*, no. February, 2018.

[19] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities." Elsevier, 2018.

[20] M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, "A review on Internet of Things (IoT), Internet of everything (IoE) and Internet of nano things (IoNT)," in *2015 Internet Technologies and Applications (ITA)*, 2015, pp. 219–224.

[21] M. M. H. Onik, N. Al-Zaben, J. Yang, and C.-S. Kim, "Privacy of Things (PoT): Personally Identifiable Information Monitoring System for Smart Homes," in *Proceedings of Symposium of the Korean Institute of communications and Information Sciences*, 2018, pp. 256–257.

[22] S. Aich, K. Muduli, M. M. H. Onik, and H.-C. Kim, "A Novel Approach to Identify the best Practices of Quality Management in SMES based on Critical Success Factors using Interpretive Structural Modeling (ISM)," *Int. J. Eng. Technol.*, vol. 7, no. 3.29, pp. 130–133, 2018.

[23] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, "Security and privacy in cyber-physical systems: A survey of surveys," *IEEE Des. Test*, vol. 34, no. 4, pp. 7–17, 2017.

[24] A. Chattopadhyay, A. Prakash, and M. Shafique, "Secure cyber-physical systems: current trends, tools and open research problems," in *Proceedings of the Conference on Design, Automation & Test in Europe*, 2017, pp. 1104–1109.

[25] N. Al-Zaben, M. M. H. Onik, J. Yang, N.-Y. Lee, and C.-S. Kim, "General Data Protection Regulation Complied Blockchain Architecture for Personally Identifiable Information Management," in *International Conference on Computing, Electronics & Communications Engineering 2018 (iCCECE '18)*, 2018, pp. 72–88.

[26] M. M. H. Onik, M. H. Miraz, and C.-S. Kim, "A Recruitment and Human Resource Management Technique using Blockchain Technology for Industry 4.0," in *Proceedings of the Smart Cities Symposium (SCS-2018)*, 2018, pp. 11–16.

[27] I. Alqassem and D. Svetinovic, "A taxonomy of security and privacy requirements for the Internet of Things (IoT)," in *Industrial Engineering and Engineering Management (IEEM), 2014 IEEE International Conference on*, 2014, pp. 1244–1248.

[28] G. D'Acquisto *et al.*, "Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics," *arXiv Prepr. arXiv1512.06000*, pp. 3928–3937, 2015.

[29] M. Hermann, T. Pentek, and B. Otto, "Design principles for industrie 4.0 scenarios," in *System Sciences (HICSS), 2016 49th Hawaii International Conference on*, 2016, pp. 3928–3937.

[30] M. M. H. Onik, N. Al-Zaben, J. Yang, N.-Y. Lee, and C.-S. Kim, "Risk Identification of Personally Identifiable Information from Collective Mobile App Data," in *International Conference on Computing, Electronics & Communications Engineering 2018 (iCCECE '18)*, 2018, pp. 71–76.

[31] H. Oh, S. Ahn, J. K. Choi, and J. Yang, "Trust visualization for object management in Internet of Things," in *Consumer Electronics, 2016 IEEE 5th Global Conference on*, 2016, pp. 1–2.

[32] A. Acquisti, "Privacy and security of personal information," in *Economics of Information Security*, Springer, 2004, pp. 179–186.

[33] P. Carey and A. Acquisti, *Data protection: a practical guide to UK and EU law*. Springer, 2004.

[34] K. Renaud, "Blaming noncompliance is too convenient: What really causes information breaches?," *IEEE Secur. Priv.*, vol. 10, no. 3, pp. 57–63, 2012.

[35] R. S. Murphy, "Property rights in personal information: An economic defense of privacy," in *Privacy*, Routledge, 2017, pp. 43–79.

Md Mehedi Hassan Onik obtained his B.S. from the Islamic University of Technology, Bangladesh. He is currently a master's candidate in the Dept. of Computer Engineering at Inje University, Korea. His research interests include data privacy, network security and blockchain technology. He is working to develop efficient personal information protection and sharing platform to handle the emerging data privacy problems.

Chul-Soo Kim is a professor in the School of Computer Engineering of Inje University in Gimhae, Korea. He received Ph.D. from the Pusan National University (Pusan, Korea) and worked for ETRI (Electronics and Telecommunication Research Institute) from 1985 - 2000 as senior researcher for developing TDX exchange. Aside from the involvement in various national and international projects, his primary research interests include network protocols, traffic management, OAM issue, and NGN charging. He is a member of ITU-T SG3, SG11, SG13 and a Rapporteur of ATM Lite from 1998 - 2002, and CEO in WIZNET from 2000 - 2001. He is currently the chairperson of BcN Reference Model in Korea, and a Rapporteur of ITU-T SG3 NGN Charging.

Jinhong Yang received Ph.D. degree form Dept. of Information and Communications Engineering at KAIST, Korea in 2017. He was Chief Technology Officer (CTO) of HECAS Inc. and developed ultra-low latency mobile video streaming technology. In March 2018, he joined at Inje University, Gimhae, Korea as an Assistant professor. His research interests include CPS, IoT and Privacy technologies.