

Aggregated Risk Modelling of Personal Data Privacy in Internet of Things

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

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

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

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

Abstract—There is a growing interest in personal data mining and user profiling to improve the surveillance practices for rapid analysis of underlying business patterns. User profiling from Personally Identifiable Information (PII) is one such technique to breach personal data privacy in mobile devices, web browser, smart homes, Internet of Things (IoT) etc. This study proposes a PII risk factor by bringing aggregated risk modelling of personal information in the IoT environment. Intuitively, most of the IoT devices are produced by identical manufacturers. Similarly, smart devices typically assemble facts from plentiful devices where collected information's owners are mutually inclusive. Proposed Massive Personal Information Clustering (MPIC) model shows that IoT product manufacturing companies can cluster PII collected from a) IoT device managing application and b) device data flow. Subsequently, owner-centric aggregated IoT device data can reveal user ID, which was not considered by other studies. Our approach was validated by satisfactory data analysis from IoT standardization organization (Open Connectivity Forum), Android and iOS app store. The analysis shows 80-90 percent of available IoT devices are manufactured by 6-10 major companies with 5 potential PII threats. Personal information like location, email, biological ID, contextual actions and social graph are at risk if collective information gathering (aggregation) through multiple IoT devices are not correctly measured. Finally, research directions in establishing privacy preservation in smart IoT ecosystem are advocated.

Keywords— Internet of Things, Data Privacy, Personally Identifiable Information, Information Security, Privacy Permission, Industry 4.0

I. INTRODUCTION

Internet of Things (IoT) integrates several physical devices, sensors and objects under a common network that can communicate and share information without any human intervention. The IoT autonomously connects Cyber-Physical system (CPS) to establish a data-driven identical platform among physically connected device to collect and exchange data [1], [2]. This higher deployment of IoT devices is expected to grow to 10 billion by 2020 and 22 billion by 2025. Intuitively, to adjust a data-driven competitive market, IoT devices frequently use Personally Identifiable Information (PII) [3], [4]. Pfizmann and Hansen [5] have termed Personally Identifiable Information (PII) “An identity is any subset of attribute values of an individual person which sufficiently identifies this individual person within any set of persons”. A

slightly different from PII, quasi-PII can be termed as Potential Personally Identifiable Information (PPII). Same author [5] defined PPII as “A partial identity is a subset of attribute values of a complete identity, where a complete identity is the union of all attribute values of all identities of this person”. Massive business chances that exist in the IoT domain meaningfully amplified the amount of smart IoT sensors and intelligent data mining and analysis in IoT.

Until now several components of this IoT sectors are well studied and analysed [6]-[9]. However, in-between data privacy, security, personal information sharing, and device trust are still in their infancy [10]. Placement of IoT devices that assemble people private data pose a new dimension of risk to individuals' privacy. Legacy privacy breaching requires actions from users. However, IoT nodes are gathering user's private information without any consent and put their privacy at stake [11]. Existing IoT privacy preserving approaches are generally user, content or context centric. However, the Internet of Things (IoT) devices are naturally developed by a specific group of companies. Currently, available devices and sensors are mostly developed by Amazon, ARM, AT & T, Samsung, Ayla Networks, Bosch, Cisco, Dell, Fujitsu, [12]. Besides object-oriented privacy model data aggregation made by manufacturing companies should be controlled and monitored. Identifying companies that may passively be collated user's PII is a huge challenge where few companies dominate the IoT device producing market [13]. Zheng [14] mentioned several personal information leaking through IoT devices in Figure 1.

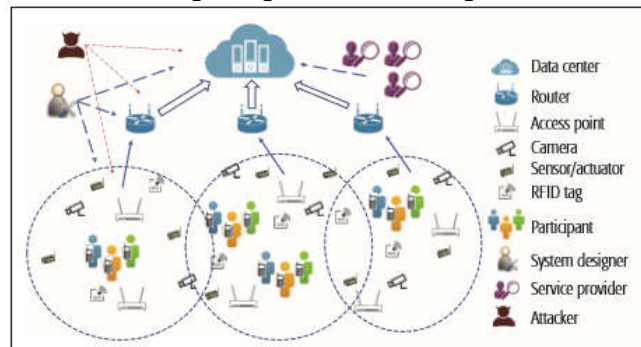


Figure 1. Information leaking in the Internet of Things (IoT) [14]

The contributions of this study in the field of protection of PII in the IoT domain are summarized as follows: (1) Risk modelling in revealing PII to a particular IoT device producing organization. (2) This study considered PII leaking to an IoT device and the ultimate owner of that information (device). (3) Possible privacy breaching options through IoT devices are identified. (4) Finally, validation is done with real data to provide insightful cautioning to the user when IoT devices from identical manufacturers are used.

II. LITERATURE REVIEW

Although people are getting conscious of securing personal information and considering those as an asset, several recent incidents have shaken the whole world in perspective of data privacy. Personal data privacy risk in IoT has been widely studied. Internet of Things (IoT) devices generally reveal sensitive personal information in two ways as below:

A. IoT Device Controlling Application:

Most of the IoT devices can be controlled by mobile applications. Generally, Android [15] and iOS [16] apps are used to control the functionalities of IoT devices. Previous studies have also provided enough evidence of personal information leaking through android privacy permissions [17], [18]. After companies introduced a cloud-based system, third parties are also developing applications for IoT devices [19]. Examples of such app are Samsung's SmartThings, Microsoft Corporation, Kakao's kakaomini, Apple's HomeKit, Vera Control's Vera3, LG, Naver's Clova, Google's Weave, AllSeen Alliance's AllJoyn, Qualcomm, Cisco and AT&T. Previously stated device handling applications gain access to all privacy permission regardless of their device functionality. The home-level granularity of IoT applications means all applications are overprivileged inevitably. Therefore, android must make a manifest template that contains individual interfaces of other apps. This manifest signifies application's permission demand like smartphone apps demand permission to sensitive resources. At installation time, the admin practices the security manager to an identity certificate [19]. Above concept is similar like smartphone owner accepting the set of permissions an app requests [15], [16] (Figure 2).

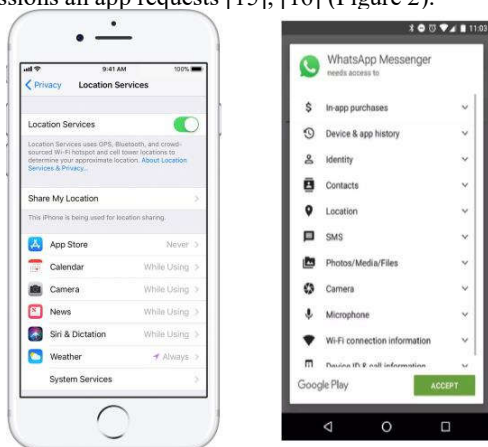


Figure 2. iOS and Android Application Privacy Permission [15], [16]

B. IoT Devices:

Another way of breaching user privacy through IoT device is service level data sharing from device to manufacturing companies. For serving device functionality IoT devices send multi-dimensional personal data either for processing or storing. Several studies have already mentioned misuses of IoT device data collection procedure [20].

C. Internet of Things (IoT) Privacy-Preserving Model

Most of the devices gather information in IoT environments have unusual properties; even some of them are without user interfaces (IoT server gather data but generates no signal). Encryption and de-identification are existing techniques to secure privacy. However, the process of achieving those in IoT is not energy and cost-effective. The General Data Protection Regulation (GDPR) [21] imposes control over personal data which also covers the data produced in IoT. Victor morel [22] mentioned two trust generating procedure. The first process was to implement transparency by connecting information gathering device and user devices. The second method to bring transparency is declared through a registry. This registry stores relevant information of data collection, devices, range and laws. Studies identified user normally choose pragmatic posture on distributing their private information [23]. An incentive can be a reasonable exchange of their private information. At this point, personal data monetization has a concrete effect on personal database-oriented research. That is, they would agree to release of some of their sensitive facts in return for few incentives. This has inspired an important drive in the database research field to monetize private information, based on potential privacy risks, and compensate users directly [24]. Privacy-Preserving Protocols for Securing a reliable data aggregation in IoT-enabled smart Systems by another study [25]. The study suggested a new protocol in Smart Grid Advanced Metering Infrastructure (AMI) to decrease issues while providing a viable privacy-preserving data collection strategy. IoTivity is an open source framework by the Open Connectivity Foundation (OCF) [26]. IoTivity's [27] aim is developing an exposed reference implementation of OCF's Internet of Things (IoT) standards to enable communication of IoT devices among themselves and the web. In this study, we will only analyse IoT devices standardized from OCF. IoTivity doesn't include security features by default.

III. PROPOSED METHOD

This section presents in detail explanation of proposed Massive Personal Information Clustering (MPIC) PII risk model.

Massive Personal Information Clustering (MPIC)

Gathering of cumulative privacy permission by particular IoT device manufacturer is a threat for any IoT user. We posit that users that have given more of PPII on IoT devices, produced by a particular manufacturer have also higher chance of exposing their PII to that device producing company. Figure 3 and Figure 4 illustrates the MPC proposition.

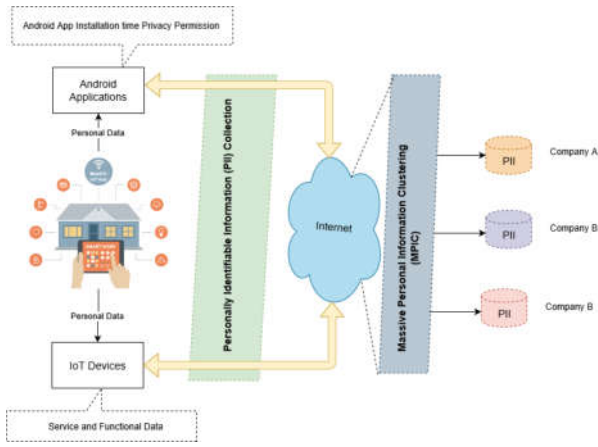


Figure 3. Massive Personal Information Clustering (MPIC)

For using an IoT device sensitive personal information (PII or PPII) is needed. This information can be collected either by application or directly by the device. In the market, millions of IoT device are there from thousands of manufacturers. We posit that users that have given more of PPII on IoT devices, bought from a particular manufacturer also poses a higher scope of revealing their PII. That is, a set of users can be defined as U_1 to U_n , set of PPII of a user U can be termed as $PPII_1$ to $PPII_n$. Let a set of IoT device manufacturer are Man_1 to Man_n . Suppose, a group of IoT device are Dev_1 to Dev_n . We explore the above conjecture to propose that if a set of information given to a particular device manufacture Man_1 is $PPII_{man1}$ to $PPII_{mann}$ through Dev_1 to Dev_n then Man_1 gets all $PPII_1$ to $PPII_n$. Therefore, Man_1 is very likely to produce PII of user U_1 by summarizing. The total PPII from a user, U_1 can be calculated by below equation. According to our proposition, user U_1 provides manufacturer Man_1 total PPII –

$$PPII = \sum_{Dev_1}^{Dev_n} PPII \quad (1)$$

If the chance of particular PII breaching through IoT device Dev_1 to Dev_n to Man_1 to Man_n are $P_a(A)$, $P_b(B)$, $P_c(C)$... $P_n(N)$. After that, the probability of breaching a specific PII for collective device information can be expressed as $P_a(A) + P_b(B) + P_c(C)$ or $P_a(A) \cup P_b(B) \cup P_c(C)$. By the way, specific Personally Identifiable Information (PII) is mutually exclusive. Therefore, the chance of leaking a particular PII to a specific manufacturer from list of manufacturers Man_1 to Man_n is independent that is, P_1 to n (A and B and C and D... N) = 0. Fig. 4 shows, user giving personal information (truly PPII) to 4 distinct devices (i.e Smart Alarm, Smart Watch, Smart Light and Smart Coffee Maker). It is seen from Fig. 4 that ‘IoT System Manufacturing Company’ is the manufacturer of all four IoT devices. At this point, if that particular manufacturing company process information from individual IoT device server for profiling, that particular manufacturing company can achieve PII of that two users.

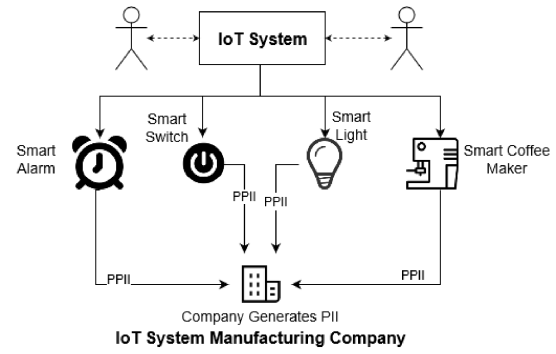


Figure 4. Gathering of Personal Information by Manufacturing Company

Rest of the section will elaborate with proposed Massive Personal Information Clustering (MPIC) step by step.

A. Product Developed by the Same Company

At present, 8.4 billion IoT devices are out there in the market but a number of established and widely used IoT manufacturing companies are meagre. User preference and trust motivates IoT users to go for a particular set of smart devices. Previously mentioned causes create a set-up where a particular user is destined to use IoT devices from a selected group of IoT device manufacturer. Figure 5 shows an example where several products from the same company.

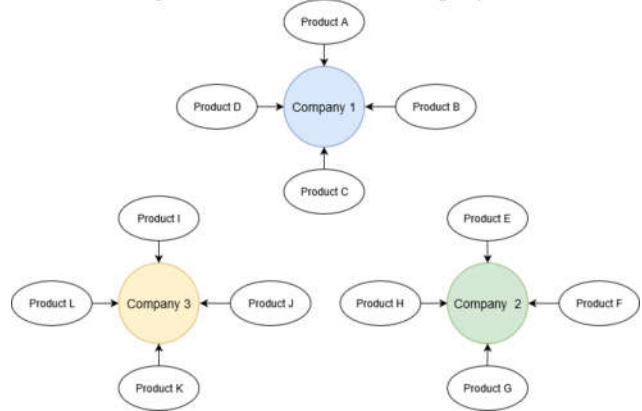


Figure 5. IoT Company's Gathering PII from their Products (Device level)

B. Device Sensing PII and PPII

Usually, IoT devices vastly collect PPII and PII for serving user and business requirements. IoT system is gathering user personal information either legally or illegally. Firstly, the IoT system can acquire user consent to collect personal data through the device's privacy permission agreement and through the device itself for maintaining service. Secondly, unexpected data breaching and information hacking by a hacker or third parties. For now, this work only focuses on the PPII gathering by IoT system manufacturer rightfully. Therefore, in connection to the last discussion IoT users are actually providing a lot of PPII to a preferred group of IoT system manufacturer. Figure 6 shows an example where several PPII and PII is connected to the same company.

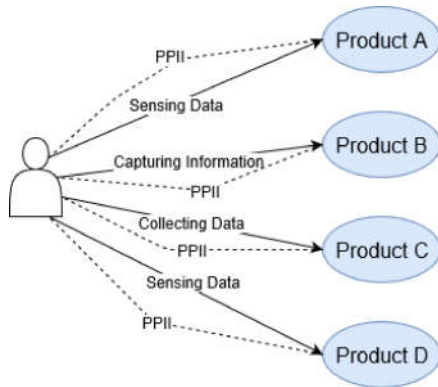


Figure 6. IoT products are sensing PPII from users.

C. Company gathering PII and PPII

Internet of Things (IoT) manufacturer uses cloud storage (servers) to store data produced by the device. Smart IoT devices frequently use those storages and update collected PII. From IoT user's viewpoint, data are given to a specific manufacturer. Contrary, if that user uses 5 devices from same users then all 5 devices are giving information to a particular company. That is how the IoT device producing manufacturer is producing enormous information indirectly. Figure 7 shows an example where several PPII is producing PII.

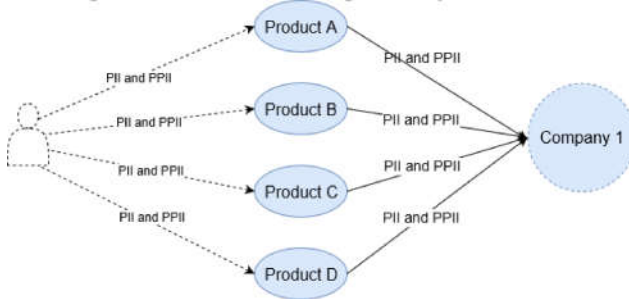


Figure 7. Company gathering PPII and PPII from products

D. Company Generates PII

At this stage, an IoT system manufacturer company who has several PPII of a particular user can easily accumulate those to generate PII. Although, an IoT manufacturing company is not collecting PII directly, indirectly a manufacturer is very likely to have the PII of their top customers. The same assumption complies with other popular IoT devices manufacture used by that user. Figure 8 shows an example where several PII of user are exposed to companies.

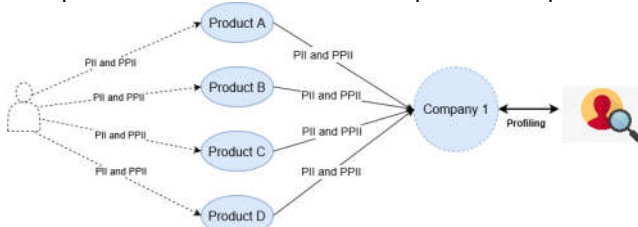


Figure 8. Profiling to generate PII by Company

E. Company Producing User Identity and Profiling

Finally, the company is having some users PII means it is actually having a huge control on those user's privacy. Since that particular company is in control of those PII is now able to misuses, sell or manipulate user information. Figure 9 shows an example where several personal information of user is exposed to companies.

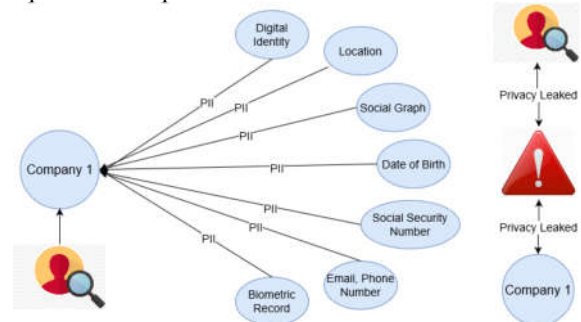


Figure 9. The company owns users personal information

IV. EXPERIMENTAL ANALYSIS

A. Dataset Collection and Analysis

This study separates the experimental analysis in two dimensions. Firstly, personal information collected through Android or iOS application. That information collected while installing or using through proper consent gathering process (privacy permission). Secondly, data producing by a particular device to serve the purpose of that particular device. To maintain the functionality of an IoT device, it often exchanges information with its server.

• Application Level

According to the computer world, UK and Forbes top IoT system manufacturing companies are HPE, IBM, Intel, Microsoft, Oracle, Qualcomm, Salesforce.com, and Samsung. In this study, we have collected 26 android and iOS application related to IoT. For Android and iOS, this study considers the dangerous permission only. This work uses, webscraper.io an open source Chrome extension was utilized to scrap data from android play store [15] and iOS store [16]. Scraper automatically visits specified web pages and dynamically developed the necessary database.

• Device Level

For evaluating device level data leaking we consider several other study resources [28] and Open Connectivity forum [26]. OCF is a worldwide famous IoT standardized organization with renown companies from around the world. This study mainly focuses the information an IoT device sends during the process device operation. Total number of Product according to OCF is 2425. However, due to the privacy issue, the Certified Product Registry contains only 105 devices. Figure 10 shows that most of the devices are manufactured by a certain group of companies. Technicolor company leading the race with 39 devices. The fact is, the company offered only 1 type of device, means the chance of using that device is also higher. Electrolux is at second position with 26 devices where they only offered 3 types.

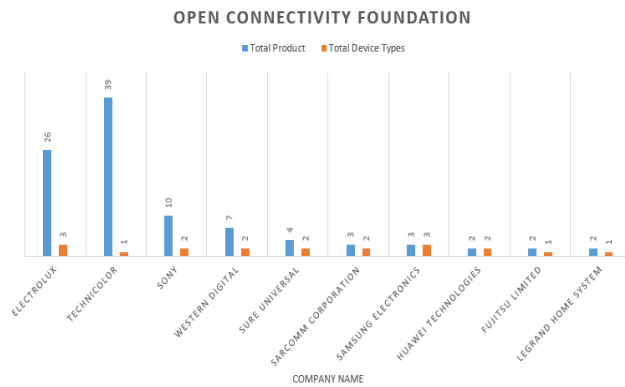


Figure 10. Manufacturer vs OCF devices

B. Model Validation

• Application Level:

Android and iOS apps used for IoT device control also release sensitive user information through application privacy permission. Manufacturing companies can aggregate personal information collected through different applications. However, Account detail, Location, Camera, Read Phone Status and External Storages are frequently taken sensitive permission. Figure 11 shows risky PII according to our MPIC method.

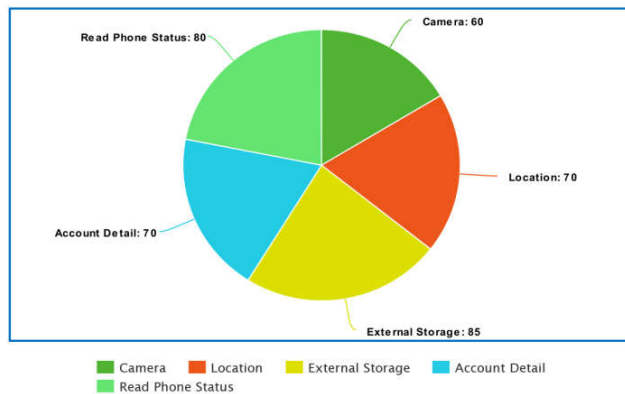


Figure 11. Risky Personally Identifiable Information (Application)

• Device Level:

According to the analysed data open Connectivity Foundation, top 5 companies produced 90% of the available certified product list. This is really a warning for user's personal data. Because, if the user keeps using those IoT devices produced from the identical manufacturing company then personal information mentioned in figure 12 are at risk. Health Status, Internet Information, Hobbies and Politics and Biological Identity are at risk through IoT device data sharing.

V. DISCUSSION AND FUTURE SCOPE

Previous experimental analysis validates our assumption about aggregated privacy risk modelling. Figure 11 and Figure 12 displays risky potential PII. At this moment, we will discuss a few research direction and existing issues related to IoT app privacy and IoT device privacy:

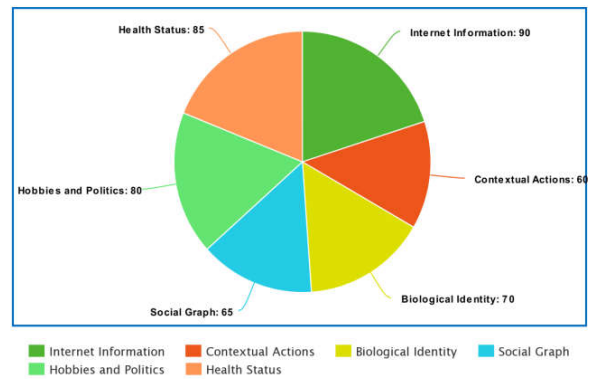


Figure 12. Risky Personally Identifiable Information (Device)

Device Privacy and Application Privacy Conflict:

Google and Apple are moderating android and iOS application privacy permissions. But, no such moderation is there for IoT device controlling application separately. IoT device itself can leak personal information while service level data sharing. So, this study recommends separate moderation of IoT device permission and IoT device controlling applications. Therefore, this study thinks IoT device sellers should gather consent from users solely for IoT device service level personal data collecting. User-managed Independent Privacy Policies: At this moment several mobile applications can manage more than one IoT devices. This allows needless permission to a specific IoT device. The user-managed sovereign privacy policy is needed. Limited scope for IoT device Certification Authority: At this moment very few IoT device certification authorities are present. Even if, certification authorities want only basic requirements from IoT device [26]. Global standardization authority is needed for securing the privacy of personal information related to IoT devices. IoT system privacy awareness: IoT system privacy awareness is required. Although several types of research have already proposed IoT privacy monitoring architecture [29], [30]. However, context-aware and aggregated risk modelling-based privacy monitoring system are still absent.

VI. CONCLUSIONS

This paper proposes a novel approach for summarizing Personally Identifiable Information (PII) leaking risk through IoT devices. Our study firmly believes IoT apps and devices, regardless of IoT device type, after clustering information can release PII. Plenty of risks generate, when PII are achieved by a specific IoT device producing company through aggregation of Potential Personally Identifiable Information (PPII) presents in cloud servers. An extensive review of personal data gathering of IoT devices with device manufacturing companies is needed for securing personal data privacy. This study requires large-scale data analysis with diverse use cases.

ACKNOWLEDGMENT

Institute for Information & communications Technology Promotion (IITP) fund this research from the grant from Korea government (Ministry of Science and ICT) (Grant

ID.2018-0-00261) titled "General Data Protection Regulation Compliant Personally Identifiable Information Management Technology for the Internet of Things Environment".

REFERENCES

- [1] 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)* pp. 219-224, 2015.
- [2] F. Tao, J. Cheng, and Q. Qi, "IIHub: An Industrial Internet-of-Things Hub Toward Smart Manufacturing Based on Cyber-Physical System", *IEEE Transactions on Industrial Informatics*, 14(5), pp.2271-2280, 2018.
- [3] Davar. Pishva, "Internet of Things: Security and privacy issues and possible solution", In *Advanced Communication Technology (ICACTION), 2017 19th International Conference on*, pp. 797-808, 2017.
- [4] H. U. Rehman, M. Asif, & M. Ahmad, "Future applications and research challenges of IoT", In *Information and Communication Technologies (ICICT), 2017 International Conference on*, pp. 68-74, 2017.
- [5] A. Pfitzmann, and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management." 2010.
- [6] M. Sain, Y.J. Kang, and H.J. Lee, "Survey on security in Internet of Things: State of the art and challenges", In *Advanced Communication Technology (ICACTION), 2017 19th International Conference on* pp. 699-704, 2017.
- [7] B. Bostami, M. Ahmed, and S. Choudhury, "False Data Injection Attacks in Internet of Things", In *Performability in Internet of Things*, pp. 47-58, 2019.
- [8] M. Almulhim, and N. Zaman, "Proposing secure and lightweight authentication scheme for IoT based E-health applications", In *Advanced Communication Technology (ICACTION), 2018 20th International Conference on*, pp. 481-487, 2018.
- [9] Z. Alansari, N.B. Anuar, A. Kamsin, S. Soomro, M.R. Belgaum, M.H. Miraz, and J. Alshaer, "August. Challenges of Internet of Things and Big Data Integration", In *International Conference for Emerging Technologies in Computing*, pp. 47-55, 2018.
- [10] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities", pp. 544-546, 2018.
- [11] J. Lopez, R. Rios, F. Bao, and G. Wang, "Evolving privacy: From sensors to the internet of things", *Future Generation Computer Systems*, 75, pp.46-57, 2017.
- [12] J. Bergman, T. Olsson, I. Johansson, and K. Rassmus-Gröhn, "An exploratory study on how Internet of Things developing companies handle User Experience Requirements", In *International Working Conference on Requirements Engineering: Foundation for Software Quality*, pp. 20-36, 2018.
- [13] M. Henze, L. Hermerschmidt, D. Kerpen, R. Häußling, B. Rumpe, and K. Wehrle, "A comprehensive approach to privacy in the cloud-based Internet of Things", *Future Generation Computer Systems*, 56, pp.701-718, 2016.
- [14] X. Zheng, Z. Cai, and Y. Li, "Data Linkage in Smart Internet of Things Systems: A Consideration from a Privacy Perspective", *IEEE Communications Magazine*, 56(9), pp.55-61, 2018.
- [15] Viennot, N., Garcia, E. and Nieh, J., 2014, June. A measurement study of google play. In *ACM SIGMETRICS Performance Evaluation Review* (Vol. 42, No. 1, pp. 221-233). ACM.
- [16] Kimbler, K., 2010, October. App store strategies for service providers. In *Intelligence in Next Generation Networks (ICIN), 2010 14th International Conference on* (pp. 1-5). IEEE.
- [17] L. Fritsch, and N. Momen, "Derived Partial Identities Generated from App Permissions", In *Open Identity Summit (OID) 2017*. Gesellschaft für Informatik, 2017.
- [18] M. M. H. Onik, N. Al-Zaben, J. Yang, N.-Y. Lee, & 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)*, pp. 71-76, 2018.
- [19] Fernandes, E., Rahmati, A., Jung, J. and Prakash, A., "Security implications of permission models in smart-home application frameworks", *IEEE Security & Privacy*, 15(2), pp. 24-30, 2017.
- [20] C.J. D'Orazio, K.K.R. Choo, and L.T. Yang, "Data exfiltration from internet of things devices: iOS devices as case studies", *IEEE Internet of Things Journal*, 4(2), pp.524-535, 2017.
- [21] P. Carey, "Data protection: a practical guide to UK and EU law. Oxford University Press, Inc.", 2018.
- [22] C. Castelluccia, M. Cunche, D. Le Métayer, and V. Morel, April. Enhancing transparency and consent in the IoT. In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* pp. 116-119, 2018.
- [23] Personal data: The emergence of a new asset class an initiative of the World Economic Forum world Economic Forum, [online] Available: www.weforum.org/reports/personal-data-emergence-new-asset-class], 2011.
- [24] C. Li, D.Y. Li, G. Miklau, and D. Suciu, "A theory of pricing private data. *Communications of the ACM*, 60(12), pp.79-86, 2017.
- [25] S. Tonyali, K. Akkaya, N. Saputro, A.S. Ulugag, and M. Nojournian, "Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled smart metering systems" *Future Generation Computer Systems*, 78, pp.547-557, 2018.
- [26] S. Park, "OCF: A new open IoT consortium", In *Advanced Information Networking and Applications Workshops (WAINA), 2017 31st International Conference on*, pp. 356-359, 2017.
- [27] J.C. Lee, J.H. Jeon, and S.H. Kim, "Design and implementation of healthcare resource model on IoTivity platform", In *Information and Communication Technology Convergence (ICTC), 2016 International Conference on* pp. 887-891, 2016.
- [28] L. Wang, and R. Ranjan, "Processing distributed internet of things data in clouds", *IEEE Cloud Computing*, 2(1), pp.76-80, 2015.
- [29] 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", *Proceedings of the Korean Institute of Communication Sciences Conference*, pp. 256-257, 2018.
- [30] 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* (pp. 1-2), 2016.



Jinhong Yang received Ph.D. degree from Dept. of Information and Communications Engineering at KAIST, Korea in 2017. He was Chief Technology Officer (CTO) of HECAS Inc. and developer of 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 Cyber-Physical System (CPS), IoT and Privacy technologies.



Chul-Soo Kim is a professor in the Dept. of Computer Engineering of Inje University, Gimhae, Korea. He received Ph.D. from the Pusan National University, Busan, Korea. He also worked at Electronics and Telecommunication Research Institute (1985 – 2000) as a senior researcher for creating TDX exchange. His research interests include data privacy, network, traffic supervision, OAM and NGN charging. He is a member of ITU-T SG3, SG11, SG13 and Rapporteur of ATM Lite from 1998 – 2002. He was also CEO in WIZNET (2000 – 2001). He is now the chairperson of BeN Reference Model in Korea.



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, Inje University, Korea. His research interests include data privacy, network security and blockchain technology. He is working to develop efficient personal data management platform to handle emerging data privacy issues.