

DATA PROTECTION IN THE INDUSTRIAL INTERNET OF THINGS

Kok-Seng Wong and Myung Ho Kim
School of Software, Soongsil University
{kswong, kmh}@ssu.ac.kr

Abstract

The advancement of low-cost sensors and Internet of Things (IoT) platforms has brought on a wave of changes in how companies deliver their products and services. The Industrial Internet of Things (IIoT) is a new industrial ecosystem that combines intelligent and autonomous machines, advanced predictive analytics, and machine-human collaboration to improve productivity, efficiency and reliability. In an increasingly competitive business environment, information is the most important asset for any industry. The integration of industrial and IoT creates various attack surfaces during data transmission, data collection, data storage, data analysis, data sharing, data outsourcing and data publishing. The loss of sensitive information and other forms of enterprise information can lead to significant financial or business losses. Furthermore, the leakage of sensitive information related to external parties (e.g., external vendors) may cause reputational damage. In this paper, we will explore the impacts of data leakage and data loss in the Industrial IoT. Several of the data protection challenges and opportunities at different data processing stages, and the impact of privacy leakage for smart manufacturing are demonstrated.

Keywords: Industrial Internet of Things (IIoT), Data Privacy Protection, Smart Manufacturing, Internet of Things (IoT)

1. INTRODUCTION

The significance of the Internet in business model innovation has increased steadily since the 1990s (Fleisch, Weinberger, & Wortmann, 2015). Each new Internet wave has given rise to new digital business model patterns, and that the biggest breakthroughs to date have been made in digital industries. The revolution of Internet of Things (IoT) has brings a great impact on existing industries such as manufacturing, energy, automotive and healthcare. To stay competitive, companies are increasingly relying on IoT technology to maximize efficiency and quality of their products and services. Manufacturing companies are now identifying new growth opportunities by adding digital services and innovation strategies to their product assortment.

The IoT provides seamless integration of physical and digital worlds through networked sensors, machine learning and big data. One of the most exciting possibilities is in industrial applications known as Industrial Internet of Things (Industrial IoT). The Industrial IoT has been heralded as a way to improve operational efficiency and reduce overall maintenance cost. The communication and interaction capabilities can be extended to devices or things used for factory and city automation, renewable energy resources, intelligent transportation systems (ITS), and vehicular communications.

According to the World Economic Forum (O'Halloran & Kvochko, 2015), *As the Industrial Internet gains broader adoption, businesses will shift from products to outcome-based services, where they compete on their ability to deliver measurable results to customers. Such outcomes may range from guaranteed machine uptimes on factory*

floors, to actual amounts of energy savings in commercial buildings, to guaranteed crop yields from a specific parcel of farmland. Delivering such outcomes will require new levels of collaboration across an ecosystem of business partners, bringing together players that combine their products and services to meet customer needs. Software platforms have emerged to better facilitate data capture, aggregation and exchange across the ecosystem."

The Industrial IoT is one of the major revolutionary technologies that have become a significant trend lately (Da Xu, He, & Li, 2014; Perera, Liu, Jayawardena, & Chen, 2014). This technology will drastically change the manner of industrial production, user-machine interaction and machine-to-machine communication. For example, sensors that monitor weather and traffic conditions help logistics managers to perform real-time traffic analysis to avoid traffic congestion. Some airplane manufacturers such as Airbus and Boeing have begun to build networked sensors into airplane bodies in order to collect continuous flight data during the entire route of the flight. The collected data will be used by the airlines to improve their proactive maintenance activities.

The market associated with the Industrial IoT has been growth tremendously over the past few years. As estimated by Gartner (Gartner, 2013), the incremental revenue generated by the IoT can reach \$309 billion per year by 2020. However, the implementation of industrial IoT technology is limited due to the interoperability challenges of device connectivity, security and privacy concerns, and convergence between technologies.

1.1 Industrial IoT Requirements

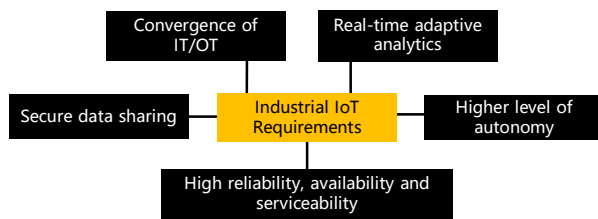


Figure 1. Industrial IoT Requirements

To realize the full opportunities presented by the Industrial IoT, it is important for companies to fulfill requirements as shown in Figure 1.

To make Industrial IoT possible, convergence between enterprise information technology (IT) infrastructure and operations technology (OT) plays an important role. Enterprise IT is needed to support customer relationship management, resource planning and decision support systems while OT is used to monitor and control field equipment, manufacturing and production processes. As reported in (Atos, 2012), IT and OT convergence provides benefits such as cost reduction, risk reduction, enhanced performance and flexibility gains to industries such as manufacturing and telecommunication. However, the integration of IT and OT is not easy because the technologies are owned and operate under different technical standards and are managed by different vendors or providers.

Real-time adaptive analytics are what enable devices or smart things in Industrial IoT to analyze and interpret enormous amounts of data. It is an important requirement in order to allow decision makers or autonomous systems to make real-time decisions during operational events and at the speed of the overall business (Brule, 2013). The adaptive analytics allow devices to identify, diagnose and report issues more precisely and hence, improve operational processes.

Sharing data with internal departments or external vendors requires secure mechanisms (e.g., access control infrastructure) to prevent information leakage. Sensitive data including the blueprints, manufacturing processes, cost information and operational data should be protected.

High level of autonomy is essential to ensure that any malfunctioning operation can be detected, recovered, reduced and maintain automatically. Autonomous self-aware, self-optimization, self-configuration and self-diagnosis systems possess the capability of configuring, healing, optimizing, and protecting operation autonomously. For example, an autonomous self-aware and adaptive fault-tolerant routing technique can be used to address the limitations of self-healing routing (SHR) and self-selective routing (SSR) techniques for routing sensor data in Industrial IoT (Abba & Lee, 2015).

High reliability, availability and serviceability (RSA) is another important requirement for Industrial IoT. A reliable

system should be able to halt any fault operation instead of silently continue to deliver results. A high available system is capable to disable the malfunctioning operation and continue operating at a reduced capacity whereas serviceability ensures fast recovery of a failed system.

In this paper, we discuss about the convergence of technologies, characteristics and requirements in IIoT (Section 2), identify security and privacy problems in existing and new Industrial IoT systems (Section 3) and provide technological solutions for data protection in Industrial IoT (Section 4). Since different industries have different data protection requirements, our discussion in this paper will be centered on the smart manufacturing.

2. SMART MANUFACTURING

Smart manufacturing is the dramatically intensified and pervasive application of networked information-based technologies throughout the manufacturing and supply chain enterprise (Davis, Edgar, Porter, Bernaden, & Sarli, 2012). It provides operators of factories, plants, supply chains and fleets with intelligence capabilities (e.g, self-aware and self-configuration) to improve performance and agility. Smart manufacturing is closely related to 4th Industrial Revolution or better known as Industry 4.0 (Drath & Horch, 2014), which is the German strategic initiative to take up a pioneering role in industrial IT. For example, a smart factory that integrates advanced and automated manufacturing facility can support production that is more efficient and provides safer approaches to manufacturing various products.

2.1 Characteristics of Smart Manufacturing

In smart manufacturing, the work content, work processes and the working environment will change significantly due to the increase of real-time oriented control. Implementation of a socio-technical approach will change the roles of each employee. The employees have the opportunity to enjoy greater responsibility and enhance their personal development (Kagermann, Wahlster, & Helbig, 2013). Individual production steps are seamlessly connected, from product development, production planning, engineering and scheduling, assembly processes, production control, through to logistics (Bartezzaghi, Cagliano, Caniato, & Ronchi, 2016).

The benefits of implementing Industrial IoT include increased production and quality, better service levels, increased network capacity, improved troubleshooting and safety, and streamlined maintenance. We summarize the major features of a smart manufacturing as follows:

Machine self-diagnosis. Sensors and other smart things can be added to new or existing plants in order to monitor exterior parameters such as temperature changes and energy consumption levels. The retrofit process allows the system to look for machine or operation that need maintenance (or are approaching failure).

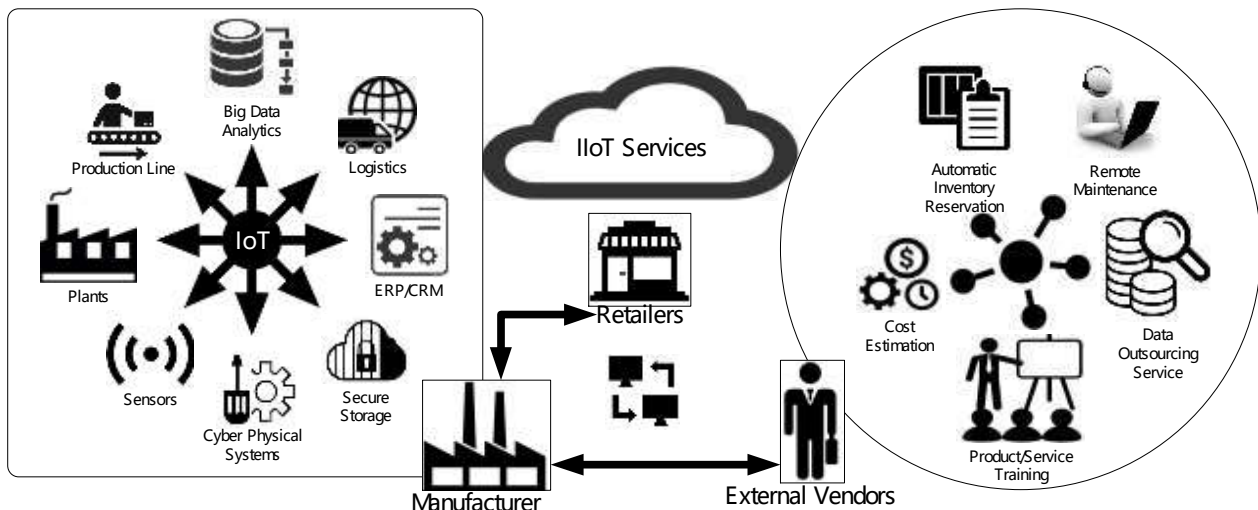


Figure 2. Industrial IoT Supported Smart Manufacturing

Remote diagnostics and maintenance. The manufacturing industry is relying on third party maintenance providers to service equipment. With Industrial IoT technologies, maintenance can be done remotely (from anywhere online) to save time and travel costs associated with checking equipment onsite.

Self-aware inventory monitoring and management. A manufacturer often relies on inventory of raw materials to complete a finished product. It is essential to understanding how much inventory it has on hand and knowing what materials it needs for upcoming projects. The self-aware inventory monitoring and management system allows the manufacturer to place an order to maintain adequate stock levels. In addition, it helps the manufacturer to plan in expectation of increasing demand or rising cost of supplies.

Connectivity. The adoption of standards for manufacturing can open new market opportunities to manufacturers. In general, vendors will support the standards for new smart equipment and connectivity methods. Following a survey results reported in (Leiva, 2016), the connectivity in smart manufacturing can be categorized into machine automation connectivity, production systems connectivity, digital thread connectivity, value chain connectivity.

Communication. Any communication between people, equipment, operational processes and enterprise to exchange information, making decision, detect and response to fault will be faster and more reliable.

Cyber physical systems. Cyber physical systems combine IT, communications, data and physical elements using core technologies such as sensors, internet communication infrastructure, big data, real-time analytics and event management.

Legacy systems upgrade. Many existing manufacturing companies have been setup and operated for many years. The implementation of industrial IoT helps companies take care of data acquisition.

2.2 Components in Smart Manufacturing

There are several key components in a smart manufacturing (as illustrated in Figure 2). We identify each of them as follows:

- Manufacturer**, a factory or company that makes goods or services.
- Retailers**, an authorized party or company that sells goods produced by the manufacturer.
- External vendors**, an external party or company that provides goods or services to the manufacturer.
- Internet of Things**, an internetworking of physical devices, objects, and smart things that embedded with sensors, software and connectivity to exchange data with business processes (over internet network) without involving human intervention.
- Sensitive information**, confidential data such as manufacturing processes, cost information, operational data, intellectual property and customer data.

3. PRIVACY LEAKAGE AND CHALLENGES

In a recent survey conducted by the World Economic Forum (O'Halloran & Kvochko, 2015), concerns on issues such as interoperability, security and privacy, Return on Investment (ROI), technology immaturity and lack of skills workers have been identified as the barriers inhibiting IoT adoption in the industrial. With the shift from industrial manufacturing to knowledge creation and service delivery,

the value of information and the need to manage it responsibly have grown dramatically (Cavoukian, 2009). As more and more devices and smart things are integrated into all aspect of industrial IoT, security and privacy become critical for the dependability of operation processes built upon these intelligent systems.

Security and privacy are two distinct but related issues in the area of information technology. The notion of security is about preventing unauthorized access to proprietary data, while privacy deals with considerations such as who own the data, who can access it, and how it can be used. In this section, we will identify privacy leakage and its challenges in smart manufacturing.

3.1 Sources of Privacy Leakage

In an increasingly competitive business environment, information is the most important asset for any manufacturer. Due to the explosion of low-cost sensors, smart devices, and IoT technology, the industrial data volume has been growing exponentially. This dramatically will increase the opportunity for theft and accidental disclosure of sensitive information (Poarch, Grahm, Park, & Martin, 2015).

Attackers often target essential and highly sensitive information such as product designs, financial data, marketing plans, customer and supplier lists, and partnership agreements. The loss of sensitive information and other forms of enterprise information can lead to significant financial or business losses. Furthermore, the leakage of sensitive information related to external parties (e.g., external vendors) may cause reputational damage.

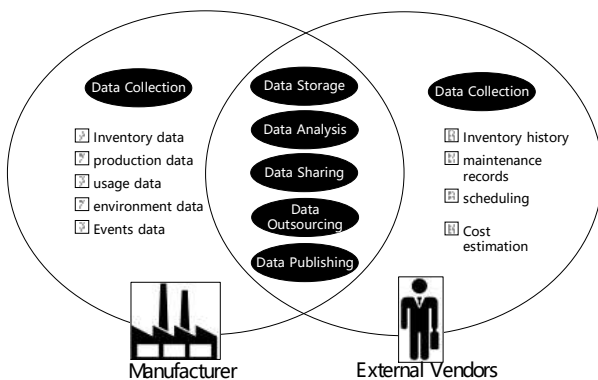


Figure 3. Data Processing in Smart Manufacturing

As shown in Figure 3, the interaction between manufacturer and external vendors involves data processing stages such as data collection, data sharing, data processing, data storage, data outsourcing and data publishing. The data generated and used at each stage can be a source of privacy leakage. In the following sections, we will identify possible cause of privacy leakage at different data processing stage.

3.1.1 Data Collection

A key objective of any manufacturing process is data collection. The ability to keep track of stock levels, order records, shipping details, and other operational data are essential to ensure that a facility or factory runs smoothly.

In an operation during a given operational period, the manufacturer may collect the following data:

- **inventory data**, information about how a particular item is configured.
- **production data**, any data related to the production line.
- **usage data**, information on how an item is operated.
- **environment data**, information about the operating conditions of an item.
- **events data**, information about event that happened to an item during its life.

Since the cost for implementation and maintaining regular data collection can be very high, the existing manufacturers generally do not have any secure mechanism to protect their raw data. We can foresee this problem in many manufacturers that already run businesses for a long period.

At the other side, external vendors may collect data such as inventory history (e.g., current and past stock levels), maintenance records (e.g., due date and maintenance service details), scheduling of maintenance, and cost estimation for each manufacturer. Often, these data have a direct relationship with the manufacturer's market strategies and business plans. Hence, it is possible for a competitor to use them to make predictions about the next movement or strategy of its targeted manufacturer.

3.1.2 Data Storage

A privacy concern arises when the cloud is used for IoT-data storage. In many cases, the data are interesting information that have been processed by the real-time analytics and represent valuable and sensitive information that should be protected. Often, cloud-service providers claim that the data they store are encrypted and private, but the manufacturers cannot verify this. They are not clear who can access, manage, and manipulate their data in the cloud storage. The privacy issue is worsened when the service providers outsource the stored data to a third party due to a lack of resources or expertise, or cost constraints. Data outsourcing places the manufacturers' data at risk because IoT data can be legally sensitive or proprietary to organizations.

3.1.3 Data Sharing

In smart manufacturing, the manufacturer can share certain information (e.g., production quantity and stock levels) with the external vendors via vendor-managed inventory (VMI) (Waller, Johnson, & Davis, 1999). Then the vendors will take full responsibility for maintaining the inventory of the material. Although vendors are creating private networks for data sharing with the manufacturer, but

there is a lack of data integrity and security mechanism to ensure the shared data are secure during data transmission and data storage at vendor site.

3.1.4 Data Analysis

The massive data generated by sensors during operational processes are rich with hidden information. Some of these data may be used automatically with other devices or applications without the manufacturer's knowledge. During the data-analytics stage, the smart devices or equipment will employ a series of analytics tools to perform real-time computations on the collected data. For instance, data-mining algorithms will be applied to extract useful information from the collected data.

3.1.5 Data Outsourcing

Complex data analytics are something that many manufacturers and vendors are still wary of investing in for fear of the expense and technical challenges they can pose. Lack of in-house expertise to conduct the data analysis causes the manufacturer or vendors to outsource the data mining activities to some external data miners. In the effort to improve the quality of the data mining result, they usually release a customized dataset that only preserves specific types of patterns for such a data mining task. Hence, the data mining activities performed by the third party can learn many sensitive information of the manufacturer.

3.1.6 Data Publishing

Publishing manufacturer's data to third parties can be at high risk because sometimes those data reveal more than was intended. For an untrusted vendor, it may attempt to publish data collected from the manufacturer. The published data may consist of sensitive information related to products or operational processes that can be linked to the manufacturer. Manufacturing data in its original form, however, typically contains sensitive information about products, and publishing such data will violate manufacturer's privacy. In data publishing, the published data should remain practically useful while privacy is preserved. The current practice in data publishing relies mainly on policies and guidelines as to what types of data can be published and on agreements on the use of published data.

4. SECURING INDUSTRIAL IOT DATA

4.1 Cryptographic Solution

Cryptography is a promising method that can be used to protect sensitive data. In 1982, Andrew Yao introduced the first two-party computation protocol (also known as the "millionaires' problem") in (Yao, 1982). He sought a way that can allow two individuals to compare their wealth without either having to reveal the extent of their wealth to each other. Since then, many secure multi-party

computation (SMC) protocols have been proposed in the literature. As proved by Goldreich et al. in (Goldreich, Micali, & Wigderson, 1987), a secure solution exists for any functionality that can be represented as a combinatorial circuit; however, the generic construction of this circuit evaluation is somehow inefficient when a large number of parties are considered because the computational cost for a large input can be very high.

4.2 Data Anonymization

Many technologies offer ways that help with the protection of privacy regarding sensitive information. Data anonymization is an interesting solution that can be used to achieve such objective. Sweeney and Samarati proposed the k -anonymity model to address the linking attack (Sweeney, 2002). The concept of k -anonymity (Samarati & Sweeney, 1998) means that each released data is indistinct from at least $(k-1)$ other data; however, according to Machanavajjhala et al., k -anonymity is vulnerable against background-knowledge attacks (Machanavajjhala, Kifer, Gehrke, & Venkitasubramaniam, 2007). Another privacy model called the "diversity model" was proposed in (Machanavajjhala, et al., 2007) to complement the k -anonymity model. This model requires the representation of the sensitive attributes in the released dataset with at least k "well-represented" values. In (Wong & Kim, 2015), a new notion known as k -anonymity has been proposed to allow the user to choose their preferred anonymity level during the data collection.







During the data collection process, the manufacturer should be aware about the information collected by the external vendors. In another hand, the external vendors need to ensure that the data they received are correct and accurate. A self-awareness data collection protocol to raise the confidence of the respondents when submitting their sensitive information was proposed in (Wong & Kim, 2014).

4.3 Privacy-by-Design Approach

The privacy protection in smart manufacturing cannot only rely on regulatory measures but it should be embedded into the system on a technological level. The adoption of principles in privacy-by-design approach (Cavoukian, 2009) can help manufacturers to protect their data in any future development. For instance, ENISA explored the concept of privacy-by-design following an engineering approach and presented eight strategies to achieve data privacy protection (ENISA, 2015). A brief overview of their proposed design strategies is summarized as follows:

Minimize: The amount of personal data that is processed should be restricted to the minimal amount possible.

Hide: Any personal data, and their interrelationships, should be hidden from plain view.

-  **Separate:** Personal data should be processed in a distributed fashion, in separate compartments whenever possible.
-  **Aggregate:** Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.
-  **Inform:** Data subjects should be adequately informed whenever personal data is processed.
-  **Control:** Data subjects should be provided agency over the processing of their personal data.
-  **Enforce:** A privacy policy compatible with legal requirements should be in place and should be enforced.
-  **Demonstrate:** The data controller needs to prove that it is able to show how the privacy policy is effectively implemented within the IT system.

A privacy-by-design framework has been proposed in (Perera, McCormick, Bandara, Price, & Nuseibeh, 2016) for assessing IoT applications and platforms.

5. CONCLUSION

The integration of people, data and intelligent machines gave a big impact on productivity, efficiency and operations of industries. Industrial IoT allows manufacturer to optimize logistics, maintain inventory levels, and prevent quality issues. In particular, it enables real-time monitoring and predictive diagnostics of assets to automatically identify maintenance and quality problems.

Industrial IoT presents a unique opportunity for many industries to aggregate and analyze massive amounts of data. In particular, usage of automated mechanisms in the processes, real-time analytics, big data, machine learning and machine-to-machine (M2M) communications can improve operations, service levels, and product quality. However, there are further aspects that need to be addressed by the research community before the companies can fully benefit from the Industrial IoT. The adoption of Industrial IoT causes the data volume growth exponentially because the sensors and smart devices will constantly generate huge amounts of data. This dramatically will increase the opportunity for theft and accidental disclosure of sensitive information. Hence, data protection is becoming an important consideration before the implementation of Industrial IoT.

6. ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2014R1A1A2058695).

7. REFERENCES

Abba, S., & Lee, J.-A. (2015). An Autonomous Self-Aware and Adaptive Fault Tolerant Routing Technique for Wireless Sensor Networks. *Sensors*, 15(8), pp. 20316-20354.

Atos. (2012). *The convergence of IT and Operational Technology*: Atos. Bartezzaghi, E., Cagliano, R., Caniato, F., & Ronchi, S. (2016). *A Journey through Manufacturing and Supply Chain Strategy Research*, Springer International Publishing, Switzerland.

Brule, M. R. (2013). Big data in exploration and production: Real-time adaptive analytics and data-flow architecture. *Proceedings of SPE Digital Energy Conference*, March 5-7, The Woodlands, Texas, USA, pp. 1-7.

Cavoukian, A. (2009). Privacy by Design-The 7 Foundational Principles. Information and Privacy Commissioner of Ontario. Retrieved September 11, 2015, from https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.

Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics*, 10(4), pp. 2233-2243.

Davis, J., Edgar, T., Porter, J., Bernaden, J., & Sarli, M. (2012). Smart manufacturing, manufacturing intelligence and demand-dynamic performance. *Computers & Chemical Engineering*, 47, pp. 145-156.

Drath, R., & Horch, A. (2014). Industrie 4.0: Hit or hype?[industry forum]. *IEEE industrial electronics magazine*, 8(2), pp. 56-58.

ENISA. (2015). Privacy and Data Protection by Design. Retrieved October 14, 2016, from <https://www.enisa.europa.eu/publications/privacy-and-dataprotection-by-design>.

Fleisch, E., Weinberger, M., & Wortmann, F. (2015). Business models and the internet of things Interoperability and Open-Source Solutions for the Internet of Things. *Proceedings of International Workshop on FP7 OpenIoT Project*, September 18, Split, Croatia, pp. 6-10.

Gartner. (2013). Gartner Says Personal Worlds and the Internet of Everything Are Colliding to Create New Markets. Retrieved September 18, 2016, from <http://www.gartner.com/newsroom/id/2621015>.

Goldreich, O., Micali, S., & Wigderson, A. (1987). How to play ANY mental game. *Proceedings of 19th ACM symposium on Theory of computing*, May 25-27, New York, NY, USA, pp. 218-229.

Kagermann, H., Wahlster, W., & Helbig, J. (2013). Securing the future of German manufacturing industry recommendations for implementing the strategic initiative INDUSTRIE 4.0. Retrieved September 25, 2016, from <http://docplayer.net/254711-Securing-the-future-of-german-manufacturing-industry-recommendations-for-implementing-the-strategic-initiative-industrie-4-0.html>.

Leiva, C. (2016). Using integration standards in smart manufacturing. Retrieved August 8, 2016 from <http://www.controleng.com/single-article/using-integration-standards-in-smart-manufacturing/5a6324fb1a1feaa8eb64a57bd59ab137.html>.

Machanavajjhala, A., Kifer, D., Gehrke, J., & Venkatasubramanian, M. (2007). l-diversity: Privacy beyond k-anonymity. *ACM Trans. Knowl. Discov. Data*, 1(1), p. 3.

O'Halloran, D., & Kvochko, E. (2015). Industrial Internet of Things: Unleashing the Potential of Connected Products and Services. Retrieved August 28, 2016, from <http://reports.weforum.org/industrial-internet-of-things/>.

Perera, C., Liu, C. H., Jayawardena, S., & Chen, M. (2014). A survey on internet of things from industrial market perspective. *IEEE Access*, 2, pp. 1660-1679.

Perera, C., McCormick, C., Bandara, A. K., Price, B. A., & Nuseibeh, B. (2016). Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms. *Proceedings of 6th International Conference on the Internet of Things*, November 7-9, New York, NY, USA, pp. 83-92.

Poarch, D., Grahm, A., Park, D., & Martin, G. (2015). 10 Reasons Why Your Organization Needs Data Loss Prevention. *IT FOCUS AREA: SECURITY*. Retrieved August 10, 2016, from <http://focus.forsythe.com/articles/19/10-Reasons-Why-Your-Organization-Needs-Data-Loss-Prevention>.

Samarati, P., & Sweeney, L. (1998). Generalizing data to provide anonymity when disclosing information (abstract). *Proceedings of 17th ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems*, June 1-4, Seattle, WA, USA, p. 188.

Sweeney, L. (2002). k-Anonymity: A model for protecting privacy. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, 10(5), pp. 557-570.

Waller, M., Johnson, M. E., & Davis, T. (1999). Vendor-managed inventory in the retail supply chain. *Journal of business logistics*, 20(1), p. 183.

Wong, K.-S., & Kim, M. H. (2014). Towards Self-Awareness Privacy Protection for Internet of Things Data Collection. *Journal of Applied Mathematics*, 9, 2014.

Wong, K.-S., & Kim, M. H. (2015). Towards a respondent-preferred k-anonymity model. *Frontiers of Information Technology & Electronic Engineering*, 16(9), pp. 720-731.

Yao, A. C. (1982). Protocols for secure computations. *Proceedings of 23rd Annual Symposium on Foundations of Computer Science (SFCS)*, June 2-3, Chicago, Illinois, pp. 160-164.

Authors



Kok-Seng Wong obtained his Ph.D. in Computer Science (major in information security) from Soongsil University, South Korea in 2012. He is currently working as an Associate Professor in the School of Software at Soongsil University. His research interests include security and data privacy, secure computation, cryptographic protocols, cloud computing and IoT related topics.



Myung Ho Kim received his Ph.D. in Computer Science from POSTECH in 1995. He has been a professor in the School of Software at Soongsil University since September 1995. He is now the Chair of the School of Software. He specialises in business intelligence, internet security, and distributed computing.