Editorial

ICSES Interdisciplinary Transactions on Cloud Computing, IoT, and Big Data (IITCIB)

Journal Homepage: http://www.i-cses.com/iitcib

Data Centric Security and Privacy Research Issues for Intelligent Internet of Things

Prof. Hyunsung Kim, PhD [a,b,‡]

[a] Department of Cyber Security, Kyungil University, Kyungbuk, Korea
[b] Department of Mathematical Sciences, Chancellor College, University of Malawi, Zomba, Malawi

[‡]This research was supported by NRF funded by the Ministry of Education (NRF-2017R1D1A1B04032598)

kim@kiu.ac.kr ✉
orcid.org/0000-0002-7814-7454

IN today’s interconnected world based on Intelligent Internet of things (IIoT), security and privacy breach can involve one or more paths to your data. Furthermore, it is no surprise that data breaches are evolving and becoming increasingly more complex. For organizations that provide vital services such as healthcare, transportation or energy, a data failure could be catastrophic. Awareness of the need for better data centric protections has grown in recent years mostly as the result of the data breaches.

This year’s security analysis report focuses on the evolution of ransomware from traditional to new applications, the cyber security implications, the customer privacy implications in their IIoT home automation and the emergence of a machine learning innovation race between attackers and defenders. We must recognize that although technologies such as machine learning, deep learning and artificial intelligence will be cornerstones of tomorrow’s cyber defenses, adversaries are working just as furiously to implement and innovate around them. It is time for researchers to act and implement effective measures to secure data against cyber-attacks. However, many do not realize that content management is the missing piece in their systems’ cyber security strategy.

Data centric security and privacy approach lets you focus on what you really need to protect rather than the information technology (IT) networks, applications and endpoints that keep small amount of your data. Data centric security and privacy allow organizations to overcome the disconnection between IT security technology and the objectives of business strategy by relating security services to the data they implicitly protect. Protecting sensitive data can take advantage of cloud computing, mobile technology and other innovations without placing your data at risk.

Traditional security and privacy defenses are no match for the mentioned data breaches that circumvent security controls and steal sensitive data. Furthermore, IT or IIoT infrastructure and sensitive data are more mobile and ubiquitous as organizations embrace cloud computing, mobility and big data analytics tools. To address the modern threats and IT or IIoT trends, we must put our efforts to innovate and devise new security and privacy approaches based on the data centric concern.

The ICSES Transactions on Cloud Computing, IoT, and Big Data (IITCIB) Journal discusses the current and future trends of research, innovation and developments in Data Centric Security and Privacy for Intelligent Internet of Things. The IITCIB Journal promotes creation of multidisciplinary multinational research teams and development of Next Generation of Intelligent Internet of Things based on Data Centric Security and Privacy solutions for today and for tomorrow.

Your regards,
Prof. Hyunsung Kim, PhD
7 Dec., 2017