This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2841049, IEEE Transactions on Industrial Informatics

Cryptographic Solutions for Industrial Internet-of-Things: Research Challenges and Opportunities

Kim-Kwang Raymond Choo, *Senior Member, IEEE*, Stefanos Gritzalis, and Jong Hyuk Park

***Abstract*— Industrial Internet of Things (IIoT) is an emerging trend, including in non-traditional technological sector (e.g. oil and gas industry). There are, however, a number of research challenges such using cryptography and other techniques to ensure security and privacy in IIoT applications and services. In this special issue, we present existing state-of-the-art advances reported by the 21 accepted papers. We then conclude the special issue with a number of potential research agenda.**

***Index Terms*— Industrial Internet of Things Security, Industrial Internet of Things Privacy, Data Encryption**

I. Introduction

Internet of Things (IoT) has broad applications, including in industry sectors that are not normally Internet connected such as Dams, Food and Agriculture, and Water and Wastewater Systems (three of 16 critical infrastructure sectors in USA), as well as adversarial settings such as battlefields (ie.g. Internet of Battlefield Things and Internet of Military Things [1,2]). IoT also has applications in surveillance, as noted by Muhammad et al. [3] in this special issue. Specifically, the authors proposed a probabilistic algorithm to encrypt keyframes before transmitting the data, in order to minimize memory and processing requirements of IoT devices. IoT also has applications in an industrial context (also referred to as Industrial Internet of Things – IIoT in the literature).

IIoT has the potential to contribute to economic growth and global competitiveness, in terms of improving productivity, efficiency, and so on. In other words, IIoT can have far-reaching impact on the operation of industries around the world. This latest wave of technological changes will generate unprecedented opportunities along with new risks to our society. For example, due to the global reach of IIoT and the capability to directly influence and/or control the physical world (e.g. devices, factories, and infrastructures), IIoT is, and will continued to be, targeted by malicious threat actors.

Encryption and other cryptographic techniques are often considered as a silver bullet to ensure security in IIoT applications and systems. However, cryptographic techniques by themselves may only ensure certain properties to be achieved (e.g. data confidentiality), and vulnerabilities may be introduced due to poor implementation within a system. In addition, there may be competing properties such as the balancing the need to preserve the privacy of data computations and efficiency, the latter a particularly important feature in resource-constrained IIoT devices.

Therefore, in the next two sections we will describe the advances presented in the papers accepted in this special issue, designed to mitigate some of the security and privacy concerns.

II. Security

Cryptographic techniques are often considered solutions to securing IIoT (and other technologies). For example, one of the many challenges in outsourcing encrypted data, such as those sourced from IIoT devices, to a centralized server or the cloud is the inability to perform arithmetic operations over the encrypted data. Hence, there has been interest in designing fully homomorphic encryption (FHE) and related solutions. In this special issue, Gai and Qiu [4] extended their prior tensor-based FHE approach to support blend arithmetic operations over real numbers. Three other related works were also presented by He et al. [5], Xu et al. [6] and Zhou et al. [7] to support secure data searching.

Ensuring a secure communication channel between IIoT devices and other systems is crucial, and one potential solution is an authentication scheme. Li et al., [8] proposed a privacy-preserving biometric-based authentication scheme, and proved its security in the random oracle model. Karati, Islam and Karuppiah [9] proposed a lightweight certificateless signature scheme to ensure data authenticity in IIoT systems. However, unlike the approach in [8], the proposed scheme is not proven secure in the random oracle model, rather it is demonstrated to be "secure against both the Type-I and Type-II adversaries under the hardness of extended bilinear strong Diffie–Hellman (BSDH) and BSDH assumptions". In [10], the authors proposed a (t, n) secret sharing-based scheme to facilitate secure information transmission between IIoT devices.

K.-K.R. Choo is with the Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249-0631, USA (e-mail: raymond.choo@fulbrightmail.org).

S. Gritzalis is with the Department of Information and Communication Systems Engineering, University of the Aegean, Greece (Email: sgritz@aegean.gr).

J. H. Park is with the Department of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech), Korea (Email: jhpark1@seoultech.ac.kr).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2841049, IEEE Transactions on Industrial Informatics

There are also times where anonymous authentication is required, and there are schemes designed to provide such a functionality such as the server-aided attribute-based signature with revocation scheme proposed in [11] and the privacy-preserving authentication and key agreement protocols for group communication in [12].

While strictly following the access policy is crucial in most applications, there might be times where previously unauthorized users need to be access encrypted data. For example, Yang, Liu and Deng [13] proposed a lightweight break-glass access control system that supports the typical attribute-based access and the more unusual break-glass access. Specifically, in the latter, a break-glass access mechanism allows one, say a medical practitioner at an overseas emergency department, to bypass the access policy to gain access to the patient's data stored in his/her home country healthcare system in order to formulate immediate treatment plan.

Blockchain is another trending research agenda, and in the context of the scope of this special issue, there has also been attempts to integrate or leverage blockchains in ensuring IoT or IIoT security [14, 15]. In this special issue, Li et al. [16] explained how a consortium blockchain can be used for secure energy trading in IIoT, and specifically in their approach an optimal pricing strategy based on Stackelberg game is proposed.

III. Privacy

Given the capability for IIoT devices and systems to capture location-related information, there is a risk of the leakage of such information. Hence, in this special issue, Yin et al. [17] proposed a mechanism satisfies differential privacy constraint to ensure location data privacy, as well as maximizing the utility of data and algorithm.

Smart grid is another area where IIoT devices (e.g. smart meters) and systems (the latter is also known as industrial control systems) are commonly found. The need to ensure the privacy of data collected, and the analysis and aggregation of such data, has been raised in the literature.

There have, unsurprisingly, been attempts to design privacy preserving data aggregation for smart grid applications such as the fog-enabled scheme proposed by Lyu et al. [18] in this special issue. The approach of Lyu et al. [18] also has two layers of encryption scheme, where one-time-password is applied at the first layer "to encrypt individual noisy measurement to achieve aggregator obliviousness" and public-key cryptography is applied at the second level for authentication.

Zhao, Yang and Sun [19] proposed a high-order clustering algorithm design to perform fast search and location of density peaks for uncovering latent data structures in IIoT big data, without compromising user privacy.

IV. Performance

In addition to security and privacy issues, there are a number of operational challenges that need to be addressed in an IIoT application [20]. For example, a group of researchers from Dalian University of Technology, China, Iowa State University, USA, and VIT University, India, proposed a synchronization scheme which is designed to minimize energy consumption and improve accuracy during synchronization of IIoT devices [21]. There have also been attempts to optimize the performance of cryptographic operations on IIoT devices, such as the proposed approach of Bakiri et al. [22] in this special issue.

Similar the smart grids focus of Lyu et al. [18], Lai, Chen and Hwang proposed an architecture to obtain data pertaining to the power from smart meters to facilitate efficient device load recognition [23]. Still on the topic of load balancing in smart grids, Lopez, Rubio and Alcaraz [24] demonstrated how cloud resources can be leveraged to predict electricity consumption using time-series forecasting, and uniformly distribute the demand over a set of available generators for load balancing.

Performance, as noted by Hu et al. [25], can be improved by making network protocols more flexible. In this special issue, Hu et al. [25] integrated "a randomized broadcast impulsive coupling scheme" with the protocol design and demonstrated the utility of such an approach using simulations.

V. Future Work

While the research presented in this special issue contributed to addressing several of the security, privacy and performance related issues pertaining to IIoT, there are plenty more research challenges and opportunities, partly due to the constant evolution of the technologies underpinning IIoT and our cyber threat landscape. Potential research agenda include:

- Lightweight encryption scheme for IIoT systems
- Lightweight cryptographic primitives for IIoT systems
- Practical attacks against IIoT systems
- System IIoT architectures and software management
- Architecture and protocol designs for IIoT
- Data integrity and access control for IIoT
- Secure middleware and cyber physical system for IIoT
- Failure detection, prediction and recovery for IIoT systems
- Experimental prototypes, performance evaluation and validation in secure and trusted IIoT systems

One observation we made in this special issue is that the proposed schemes presented in the accepted papers generally used simulations to evaluate the performance of the schemes. We posit the importance of bridging research and practice, such as designing secure yet real-world efficient cryptographic and security solutions. Therefore, it is important for researchers to collaborate with the relevant industry stakeholders to collaboratively design and evaluate future solutions.

References

J. H. Park was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No.2016R1A2B4011069).

REFERENCES

[1] Aniello Castiglione, Kim-Kwang Raymond Choo, Michele Nappi, Stefano Ricciardi. Context Aware Ubiquitous Biometrics in Edge of Military Things. IEEE Cloud Computing 4(6): 16-20 (2018)

[2] Amin Azmoodeh, Ali Dehghantanha, Kim-Kwang Raymond Choo. Robust Malware Detection for Internet of (Battlefield) Things Devices Using Deep Eigenspace Learning. IEEE Transactions on Sustainable Computing (2018)

[3] Khan Muhammad, Rafik Hamza, Jamil Ahmad, Jaime Lloret, Haoxiang Wang, Sung Wook Baik. Secure Surveillance Framework for IoT Systems Using Probabilistic Image Encryption. IEEE Transactions on Sustainable Computing (2018)

[4] Keke Gai, Meikang Qiu. Blend Arithmetic Operations on Tensor-Based Fully Homomorphic Encryption Over Real Numbers. IEEE Transactions on Industrial Informatics (2018)

[5] Debiao He, Mimi Ma, Sherali Zeadally, Neeraj Kumar, Kaitai Liang. Certificateless Public Key Authenticated Encryption With Keyword Search for Industrial Internet of Things. IEEE Transactions on Industrial Informatics (2018)

[6] Peng Xu, Shuanghong He, Wei Wang, Willy Susilo, Hai Jin. Lightweight Searchable Public-Key Encryption for Cloud-Assisted Wireless Sensor Networks. IEEE Transactions on Industrial Informatics (2018)

[7] Rang Zhou, Xiaosong Zhang, Xiaojiang Du, Xiaofen Wang, Guowu Yang, Mohsen Guizani. File-Centric Multi-Key Aggregate Keyword Searchable Encryption for Industrial Internet of Things. IEEE Transactions on Industrial Informatics (2018)

[8] Xiong Li, Jianwei Niu, Md Zakirul Alam Bhuiyan, Fan Wu, Marimuthu Karuppiah, Saru Kumari. A Robust ECC-Based Provable Secure Authentication Protocol With Privacy Preserving for Industrial Internet of Things. IEEE Transactions on Industrial Informatics (2018)

[9] Arijit Karati, SK Hafizul Islam, Marimuthu Karuppiah. Provably Secure and Lightweight Certificateless Signature Scheme for IIoT Environments. IEEE Transactions on Industrial Informatics (2018)

[10] Jian Shen, Tianqi Zhou, Xingang Liu, Yao-Chung Chang. A Novel Latin-Square-Based Secret Sharing for M2M Communications. IEEE Transactions on Industrial Informatics (2018)

[11] Hui Cui, Robert H. Deng, Joseph K. Liu, Xun Yi, Yingjiu Li. Server-Aided Attribute-Based Signature With Revocation for Resource-Constrained Industrial-Internet-of-Things Devices. IEEE Transactions on Industrial Informatics (2018)

[12] Mingjun Wang, Zheng Yan. Privacy-Preserving Authentication and Key Agreement Protocols for D2D Group Communications. IEEE Transactions on Industrial Informatics (2018)

[13] Yang Yang, Ximeng Liu, Robert H. Deng. Lightweight Break-Glass Access Control System for Healthcare Internet-of-Things. IEEE Transactions on Industrial Informatics (2018)

[14] Mandrita Banerjee, Junghee Lee, Kim-Kwang Raymond Choo. A blockchain future to Internet of Things security: A position paper. Digital Communications and Networks (2018)

[15] Christian Esposito, Alfredo De Santis, Genny Tortora, Henry Chang, Kim-Kwang Raymond Choo. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? IEEE Cloud Computing 5(1): 31-37 (2018)

[16] Zhetao Li, Jiawen Kang, Rong Yu, Dongdong Ye, Qingyong Deng, Yan Zhang. Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things. IEEE Transactions on Industrial Informatics (2018)

[17] Chunyong Yin, Jinwen Xi, Ruxia Sun, Jin Wang. Location Privacy Protection Based on Differential Privacy Strategy for Big Data in Industrial Internet of Things. IEEE Transactions on Industrial Informatics (2018)

[18] Lingjuan Lyu, Karthik Nandakumar, Ben Rubinstein, Jiong Jin, Justin Bedo, Marimuthu Palaniswami. PPFA: Privacy Preserving Fog-Enabled Aggregation in Smart Grid. IEEE Transactions on Industrial Informatics (2018)

[19] Yaliang Zhao, Laurence T. Yang, Jiayu Sun. A Secure High-Order CFS Algorithm on Clouds for Industrial Internet of Things. IEEE Transactions on Industrial Informatics (2018)

[20] Christian Esposito, Aniello Castiglione, Francesco Palmieri, Alfredo De Santis. Integrity for an Event Notification Within the Industrial Internet of Things by Using Group Signatures. IEEE Transactions on Industrial Informatics (2018)

[21] Tie Qiu, Yushuang Zhang, Daji Qiao, Xiaoyun Zhang, Mathew L. Wymore, Arun Kumar Sangaiah. A Robust Time Synchronization Scheme for Industrial Internet of Things. IEEE Transactions on Industrial Informatics (2018)

[22] Mohammed Bakiri, Christophe Guyeux, Jean-Francois Couchot, Luigi Marangio, Stefano Galatolo. A Hardware and Secure Pseudorandom Generator for Constrained Devices. IEEE Transactions on Industrial Informatics (2018)

[23] Chin-Feng Lai, Shih-Yeh Chen, Ren-Hung Hwang. A Resilient Power Fingerprinting Selection Mechanism of Device Load Recognition for Trusted Industrial Internet of Things. IEEE Transactions on Industrial Informatics (2018)

[24] Javier Lopez, Juan E. Rubio, Cristina Alcaraz. A Resilient Architecture for the Smart Grid. IEEE Transactions on Industrial Informatics (2018)

[25] Bin Hu, Zhi-Hong Guan, Naixue Xiong, Han-Chieh Chao. Intelligent Impulsive Synchronization of Nonlinear Interconnected Neural Networks for Image Protection. IEEE Transactions on Industrial Informatics (2018)