Future Generation Computer Systems 107 (2020) 1140–1142

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Intelligent security and optimization in Edge/Fog Computing

Meikang Qiu [a], Sun-Yuan Kung [b], Keke Gai [c]

[a] *Department of Electrical Engineering, Columbia University, New Year, NY 10007, USA*
[b] *Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA*
[c] *School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China*

ARTICLE INFO

Keywords:
Edge/Fog Computing
Cybersecurity
Decentralized cloud
Artificial intelligence
Editorial

ABSTRACT

Edge/Fog Computing enables mobility support, location awareness and low latency by offloading cloud resources and services to the edge. Researchers and practitioners have embraced Edge/Fog Computing as a new approach that has the potential for a profound impact in our daily life and world economy. Particularly, security and privacy protection is a critical concern in the development and adoption of Edge/Fog Computing. To avoid system fragility and defend against vulnerabilities exploration from cyber attacker, various cyber security techniques and tools have been developed for Edge/Fog systems. This special issue focuses on the challenging topic of Intelligent Security and Optimization in Edge/Fog Computing and invites the state-of-the-art research results.

1. Introduction

Cloud computing, as the predecessor of edge computing, has been developed rapidly in the past decade. It offers users infinite computing resource as “Everything-as-a-Service” [1–3] pattern. By using cloud services, users can access relatively cheap computation resource by their demand from cloud data centers. However, such centralized setting might suffered from single point failure, and high amount of data generated at the edge of the network would cause network traffics as they uploaded to the cloud [4].

To tackle this problem, researchers proposed a novel scheme, which execute the computation task near the edge of the network [5,6], to reduce the network traffic and computing pressure on cloud data centers. By this effort, light but substantial computation tasks generated by IoT devices can be solved in a real-time way [7,8]. Edge computing carried out at the edge of the network, which fully utilized idling computing resource of edge device to address the computation task locally. When it comes to fog computing, cloudlets between cloud data centers and users handle computation tasks. In short, edge/fog computing are essential in speeding up the IoT network. Compared to the cloud, edge/fog computing are facing the challenge in deficiency of the available computation resource.

However, edge/fog computing paradigm are under different kinds of threats. First of all, as consumer electronics devices, edge devices are designed under economic consideration. Accordingly, these devices are too energy and function constrained to implement current security approaches [9,10]. Second, edge layer of the network cannot be fully controlled and supervised by service providers. Therefore, edge devices are exposed to highly dynamic and hazardous environments that attract attackers [11]. Third, communications between edge devices are also frail to be compromised. If edge devices were to connect the malicious public Wi-Fi [5], they would be remotely controlled by attackers. Last but not least, data collected by IoT devices might be misused by the honest-but-curious service provider [12]. Thus, edge devices are not be fully protected, lack of control by the user end and vulnerable to threat agents. The security challenge in edge/fog computing has been markedly impeded the development and application of this next-generation computing scheme.

As a leading technology that have a profound impact on the world, intelligent algorithms powering security assurance technique and optimization technique can surely benefit the edge/fog computing [13,14]. Combining these innovative technologies can not only promoting interactions between disciplines, but also bridging academia and industrial. Therefore, this special issue is organized to collect the novel researches in security/ optimization topic, then evaluate, discuss and improve the solutions that address the security issue in edge/fog computing.

This special issues had accepted 8 high quality papers. Each accepted paper has been assessed by a careful review and evaluation process. The decision consider both research quality and dimension balance. The special issue presents innovative solutions and showing advances on security, policy, model and architecture in edge/fog computing; privacy in network deployment and

E-mail addresses: qiumeikang@gmail.com (M. Qiu), kung@Princeton.edu (S.-Y. Kung), gaikeke@bit.edu.cn (K. Gai).

https://doi.org/10.1016/j.future.2019.06.002
0167-739X/© 2020 Published by Elsevier B.V.

management in edge/fog computing and Computational forensics in edge/fog computing.

2. Special issue contents

This special issue of the Future Generation Computer System Journal gathered papers by open call. Papers selected in this special issue were published in FGCS Journal in 2018, from volume 85 to volume 90. As we have shown below, papers selected into this special issue were in high quality and covered multiple significant aspects, going from the more traditional cartographical algorithm to machine learning based threat detection algorithm.

In the paper "Compulsory traceable cipher text-policy attribute-based encryption against privilege abuse in fog computing" [15], authors focused on how to address the privilege abuse problem in cipher text-policy attribute-based encryption (CA-ABE) under fog environment. This term was firstly proposed in this paper, which referred to the unauthorized access to fog data by the aid of malicious users. There were two kinds of privilege abuse. One kind of abuse was caused by illegal sharing of user's attribute key to unauthorized users, which leaded to unauthorized access to the sensitive data on fog node. Another kind of abuse was a result of illegal sharing the decryption device to unauthorized users, which the sensitive cipher-text were under threat. Besides, unauthorized users by the aid of privilege abuse cannot be traced and monitored.

To address this problem, Qiao [15] proposed a novel black box traceable CP-ABE scheme to track the action of malicious users. Tracing cipher-text was designed to find out the decryption key, which was used to build the decryption black box. Therefore, providers could identify the owner of this blackbox. In addition, authors proposed compulsory traceability concept as a measure whether the designed cipher-text can be distinguished from normal cipher-text by malicious users. The proposed approach was proved to be compulsory and be scalable and light-weighted to fit the fog environment.

With the rapid development of data science and machine learning, plenty of research interests were focused on the biometric based authentication system instead of traditional role based or attribute based system. While the biological data ensures the security of the whole system, users' personal data was collected and uploaded for identifying, which could be harm to users privacy. The paper "Edge-centric multimodal authentication system using encrypted biometric templates" [16] discussed the dilemma above and designed a system to solve it. First, this system concentrate on the accurate biometric authentication. Speech recognition was evaluated by Mel-frequency cepstral coefficients and perceptual linear prediction coefficients, and facial recognition was measured by eigenfaces. These three metrics then vote to decide the authentication decision. From user data privacy perspective, data was encrypted after collected by edge devices to provide data privacy and security.

The work "PrivBox: Verifiable decentralized reputation system for online marketplaces" [17] also paid attention to the user's privacy data that collected at the edge of network. The traditional online reputation system was designed in a form of centralized trusted system, which could leak the user's sensitive information in user's feedback comments. In this work, PrivBox, a decentralized reputation system was proposed. Homomorphic cryptographic system cooperated with non-interactive zero-knowledge proof to ensure data privacy and wellformedness with low computation complexity.

"Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model" [18] surveyed about existing methods in protection of new distributed and heterogeneous cybersystems. In the paper, authors first elaborated deficiency in security parameter model for edge/fog computing. Then challenges and future trends in edge/fog computing were discussed. Particularlly, distributed system architectures developed from verticals to horizontal was fully discussed and divided into three logical layers. Finally, a threat detection framework was proposed at the end of this article.

In paper "Secure data deduplication using secret sharing schemes over cloud" [19], authors studied in the area of data security under cloud data dedeuplication process. Data deduplication could delete the redundant information to increase cloud storage utilization ratio. Nonetheless, current deduplication approaches in managing convergent key faced single point vulnerability. To tackle this problem, both convergent key information and content information obfuscated into multiple shared based on Chinese Remainder Theorem. Extensive researches proved that their model could resist single point failure and ensure data confidentially and integrity. Besides, their model showed 24% percent of deduplication rate that outperformed existing state-of-the-art performance.

Instead of constructing the protection mechanism of user's data security, some models were initiatively recognizing the threat agent and proposed punishment to malware automatically. Paper "Identifying cyber threats to mobile-IoT applications in edge computing paradigm" [20], by Abawajy et al. provided a mobile malware detection model. This paper began with the survey about the malware problem, current state of mobile security and novel mobile malware. Then they listed existing approaches about dynamic and static malware analysis. One major challenge in malware detection under mobile environment was the permission abused problem of smart phone software. These software, if granted permissions to access camera or memory, could cause user's privacy leakage. Authors in this paper designed a malware classifier, where feature extractor and discriminator were trained under high volume of labeled data. Evaluations carried out showed this model could effectively distinguish the malware.

Similarity, Homayoun's work "DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer" [21] utilized machine learning technology to detect malware. In this work, they paid attention to countermeasure the ransomware, which encrypted user's personal data and carried out extortion. This virus was hazardous to sensitive data stored in fog nodes. Hence, Deep Ransomware Threat Hunting and Intelligence System (DRTHIS) model was proposed to classify not only ransomware and normal software, but also different kinds of ransomware in a short time. The deep neural network deployed in this paper consisted both convolutional neural network and pre-trained long short-term memory network. In addition, softmax layer was used to produce final classification result. Experimental results shown the pre-trained LSTM was preferred than CNN in this detecting task. Using the deep learning technology for malware detection would become next research hotspot.

Additionally, edge/fog computing could be used to support the wearable medical electronic devices. Due the low latency characteristic of fog computing, fog-based medical system was outstanding in its rapid response and energy preserving. In paper "Optimization of signal quality over comfortability of textile electrodes for ECG monitoring in fog computing based medical applications" [22], authors designed a novel fog-based wearable electrocardiogram (ECG) signals monitoring system. Textile electrodes were employed to optimize the EEG signal quality with high signal-to-noise-ratio.

Acknowledgments

We are grateful to all authors, anonymous reviewers and editors for their efforts to this special issue. We hope that the achievements gathered in this special issue will be of timely value to the community of cloud computing and readers of Future Generation Computer Systems.

References

[1] A. Ferrer, J. Marquès, J. Jorba, Towards the decentralised cloud: Survey on approaches and challenges for mobile, ad hoc, and edge computing, ACM Comput. Surv. 51 (6) (2019) 111.

[2] K. Gai, M. Qiu, Z. Xiong, M. Liu, Privacy-preserving multi-channel communication in edge-of-things, Future Gener. Comput. Syst. 85 (2018) 190–200.

[3] K. Gai, Y. Wu, L. Zhu, L. Xu, Y. Zhang, Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks, IEEE Internet Things J. PP (99) (2019) 1–13.

[4] K. Gai, M. Qiu, H. Zhao, Energy-aware task assignment for mobile cyber-enabled applications in heterogeneous cloud computing, J. Parallel Distrib. Comput. 111 (2018) 126–135.

[5] W. Shi, J. Cao, Q. Zhang, Y. Li, L. Xu, Edge computing: Vision and challenges, IEEE Internet Things J. 3 (5) (2016) 637–646.

[6] K. Gai, M. Qiu, H. Zhao, L. Tao, Z. Zong, Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing, J. Netw. Comput. Appl. 59 (2016) 46–54.

[7] P. Zhang, J. Liu, F. Yu, M. Sookhak, M. Au, X. Luo, A survey on access control in fog computing, IEEE Commun. Mag. 56 (2) (2018) 144–149.

[8] M. Qiu, M. Zhong, J. Li, K. Gai, Z. Zong, Phase-change memory optimization for green cloud with genetic algorithm, IEEE Trans. Comput. 64 (12) (2015) 3528–3540.

[9] M. Qiu, K. Gai, B. Thuraisingham, L. Tao, H. Zhao, Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry, Future Gener. Comput. Syst. 80 (2018) 421–429.

[10] K. Gai, M. Qiu, Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers, IEEE Trans. Ind. Inf. 14 (8) (2018) 3590–3598.

[11] K. Gai, M. Qiu, Z. Ming, H. Zhao, L. Qiu, Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks, IEEE Trans. Smart Grid 8 (5) (2017) 2431–2439.

[12] K. Gai, K. Choo, M. Qiu, L. Zhu, Privacy-preserving content-oriented wireless communication in internet-of-things, IEEE Internet Things J. 5 (4) (2018) 3059–3067.

[13] K. Gai, M. Qiu, Reinforcement learning-based content-centric services in mobile sensing, IEEE Netw. 32 (4) (2018) 34–39.

[14] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, Y. Zhang, Blockchain for secure and efficient data sharing in vehicular edge computing and networks, IEEE Internet Things J. (2018).

[15] H. Qiao, J. Ren, Z. Wang, H. Ba, H. Zhou, Compulsory traceable ciphertext-policy attribute-based encryption against privilege abuse in fog computing, Future Gener. Comput. Syst. 88 (2018) 107–116.

[16] Z. Ali, M. Hossain, G. Muhammad, I. Ullah, H. Abachi, A. Alamri, Edge-centric multimodal authentication system using encrypted biometric templates, Future Gener. Comput. Syst. 85 (2018) 76–87.

[17] M. Azad, S. Bag, F. Hao, PrivBox: Verifiable decentralized reputation system for online marketplaces, Future Gener. Comput. Syst. 89 (2018) 44–57.

[18] R. Rapuzzi, M. Repetto, Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model, Future Gener. Comput. Syst. 85 (2018) 235–249.

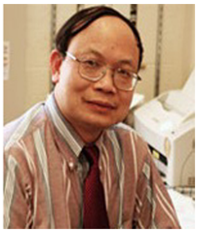
[19] P. Singh, N. Agarwal, B. Raman, Secure data deduplication using secret sharing schemes over cloud, Future Gener. Comput. Syst. 88 (2018) 156–167.

[20] J. Abawajy, S. Hudal, S. Sharmeen, M. Hassan, A. Almogren, Identifying cyber threats to mobile-IoT applications in edge computing paradigm, Future Gener. Comput. Syst. 89 (2018) 525–538.

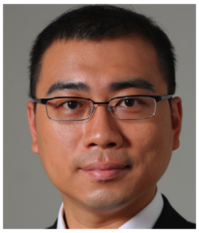
[21] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, R. Khayami, K.-K.R. Choo, D.E. Newton, DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer, Future Gener. Comput. Syst. 90 (2019) 94–104.

[22] W. Wu, S. Pirbhulal, A. Sangaiah, S. Mukhopadhyay, G. Li, Optimization of signal quality over comfortability of textile electrodes for ECG monitoring in fog computing based medical applications, Future Gener. Comput. Syst. 86 (2018) 515–526.

Meikang Qiu received the BE and ME degrees from Shanghai Jiao Tong University and received Ph.D. degree of Computer Science from University of Texas at Dallas. Currently, he is affiliated with Columbia University and is a distinguished professor at Shenzhen University. He is an IEEE Senior member and ACM Senior member. He is the Chair of IEEE Smart Computing Technical Community. His research interests include Cyber Security, Big Data Analysis, Cloud Computing, Smarting Computing, Intelligent Data, Embedded systems, etc. He has published 5 text books, 450+ peer-reviewed journals and conference papers. He has won the Middle Career Award from IEEE Computer Society (CS) Technical Committee on Scalable Computing (TCSC) in 2018. His paper published in IEEE Transactions on Computers about privacy protection for smart phones has been selected as a Highly Cited Paper in 2017 and 2018 from the Web of Science. His paper about data allocation for hybrid memory has been published in IEEE Transactions on Computers has been selected as a Hot Paper (1 in 1000 papers) in 2017. His paper on Tele-health system has won IEEE System Journal 2018 Best Paper Award. He also won ACM Transactions on Design Automation of Electrical Systems (TODAES) 2011 Best Paper Award. He has won another 10+ Conference Best Paper Awards in recent years. Currently he is an associate editor of 10+ international journals, including IEEE Transactions on Computers and IEEE Transactions on Cloud Computing. He has served as leading guest editor for IEEE Transactions on Dependable and Secure Computing (TDSC), special issue on Social Network Security. He is the General Chair/Program Chair of a dozen of IEEE/ACM international conferences, such as IEEE TrustCom, IEEE BigDataSecurity, IEEE CSCloud, and IEEE HPCC. He has won Navy Summer Faculty Award in 2012 and Air Force Summer Faculty Award in 2009. His research is supported by US government such as NSF, NSA, Air Force, Navy and companies such as GE, Nokia, TCL, and Cavium.



Sun-Yuan Kung was born in Taiwan on January 2, 1950. He received the B.S. in Electrical Engineering from the National Taiwan University in 1971; M.S. in Electrical Engineering from the University of Rochester in 1974; and Ph.D. in Electrical Engineering from Stanford University in 1977. From 1977 to 1987, he was on the faculty of Electrical Engineering-Systems at the University of Southern California. In 1984, he was a Visiting Professor at Stanford University and later in the same year, a visiting professor at the Delft University of Technology. Since September 1987, he has been a Professor in the Department of Electrical Engineering, Princeton University. He currently serves on the IEEE Technical Committees on VLSI Signal Processing and Neural Networks and an Editor-in-Chief of Journal of VLSI Signal Processing. Membership in Societies: IEEE (Life Fellow), ACM (Member).



Keke Gai received a Ph.D. degree in Computer Science from the Department of Computer Science at Pace University, New York, USA. He also holds degrees from Nanjing University of Science and Technology (BEng), The University of British Columbia (MET) and Lawrence Technological University (MBA and MS). He is currently an Associate Professor in the School of Computer Science and Technology at Beijing Institute of Technology, Beijing, China. Keke Gai has published more than 90 peer-reviewed journals or conference papers, 30+ journal papers (including ACM/IEEE Transactions), and 50+ conference papers. He has been granted five IEEE Best Paper Awards (IEEE TrustCom'18, IEEE HPCC'18, IEEE SSC'16, IEEE CSCloud'15, IEEE BigDataSecurity'15) and two IEEE Best Student Paper Awards (SmartCloud'16, HPCC'16) by IEEE conferences in recent years. His paper about cloud computing has been ranked as the "Most Downloaded Articles" of Journal of Network and Computer Applications (JNCA). He is involved in a number of professional/academic associations, including ACM and IEEE. His research interests include cloud computing, cyber security, combinatorial optimization, edge computing, and blockchain. He has served as a program chair in a number of international conferences, such as SmartBlock 2018, SmartCom 2018, HPSC 2018, EdgeCom 2018, etc.