Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 9373961, 3 pages
https://doi.org/10.1155/2018/9373961

Editorial

Security and Privacy Challenges for Internet-of-Things and Fog Computing

Ximeng Liu,[1,2] **Yang Yang**,[2] **Kim-Kwang Raymond Choo**,[3] **and Huaqun Wang**[4]

[1]*School of Information Systems, Singapore Management University, Singapore 188065*
[2]*College of Mathematics and Computer Science, Fuzhou University, Fuzhou 350116, China*
[3]*College of Business, The University of Texas at San Antonio, San Antonio, TX 78249, USA*
[4]*School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China*

Correspondence should be addressed to Ximeng Liu; snbnix@gmail.com

Received 5 September 2018; Accepted 5 September 2018; Published 24 September 2018

1. Introduction

Internet-of-Things (IoT) has been considered as a necessary part of our daily life with billions of IoT devices collecting data through wireless technology and can interoperate within the existing Internet infrastructure. The new fog computing paradigm allows storing and processing data at the network edge or anywhere along the cloud-to-endpoint continuum, and it also overcomes the limitations of IoT devices and allows us to design a far more capable architecture. Unfortunately, this new IoT-Fog paradigm faces many new security and privacy issues, such as secure communication, authentication and authorization, and information confidentiality. Although the traditional cloud-based platform can even use heavyweight cryptosystem to enhance the security, it cannot be performed on the resource-constrained fog devices directly. Moreover, millions of smart fog devices are wildly distributed and located in different areas, which increases the risk of being compromised by some malicious parties.

To address these arising challenges and opportunities different from traditional cloud-based architecture, all the papers chosen for this special issue represent recent progress in the field of security and privacy techniques relevant to the convergence of IoT with fog computing, including identity/attribute-based cryptography, system and software security, system and resource optimization, user privacy preservation, and data protection. Overall, our international editorial committee selected 17 papers among 70 submissions from both the theoretical and the practical side. All of these papers in this special issue not only provide novel ideas and state-of-the-art techniques in the field of IoT-Fog computing but also stimulate future research in the IoT-Fog computing environment.

2. Identity/Attribute-Based Cryptography

Identity-based cryptography is an attractive branch of public key cryptography which uses the public known information (such as, an email address or a physical IP address) as the public key. It arises more security and performance issues when meeting the IoT-Fog computing applications. The paper by Q. Wang et al., entitled "An Anonymous Multireceiver with Online/Offline Identity-Based Encryption", presented anonymous multireceiver online/offline identity-based encryption which could reduce the computational cost according to the online/offline encryption method suitable for the sender which had limited resources, such as mobile devices and sensor nodes. The paper by L. Zhu et al., entitled "An Efficient Identity-Based Proxy Blind Signature for Semioffline Services", presented a new proxy blind signature based on the mathematical structure called NTRU lattice, which could be independent of public key infrastructure and secure against quantum computers attack and was suitable for semioffline e-payment system and e-voting in the fog computing scenario. The proposed scheme has proven secure, that is, strongly identifiable and strongly undeniable. The

paper by W. Liu et al., entitled "Strong Identity-Based Proxy Signature Schemes, Revisited", introduced a practical attack; that is, malicious adversary can create a proxy signature on a message, if the adversary had access to the standard signature of the original signer and proxy signer. This attack had not been considered by the existing identity-based proxy signature schemes, which is greatly important for the IoT-Fog computing. Also, the authors proposed a construction that can effectively prevent this attack by transforming "normal" proxy signature scheme into "strong" one. As the extension of the identity-based cryptography, attributed-based cryptosystem can support secure one-to-many message transmission and fine-grained access control. The paper by Q. Li et al., entitled "Traceable Ciphertext-Policy Attribute-Based Encryption with Verifiable Outsourced Decryption in eHealth Cloud", presented a verifiable and traceable CP-ABE scheme in eHealth cloud. The proposed system could support the verifiable outsourced decryption and white-box traceability at the same time and could ensure the privacy of the user's identity. Also, the authors gave a delegation method to let the resource-limited devices (especially fit for the IoT-Fog computing) authorize someone else to interact with the cloud decryption server which is secure, efficient, and practical.

3. System and Software Security

System and software security is a crucial component to a device operating at its optimum from authentication and anti-virus protection to vulnerability exploitation and modifications. The system and software contain more security issues when meeting the real IoT-Fog devices. For wildly used Android devices, Z. Peng et al. gave a paper entitled "Hydra-Bite: Static Taint Immunity, Split, and Complot Based Information Capture Method for Android Device." The authors researched the Android system's application layer to use the permission split and reconstruct module to split traditional privacy stealing Trojan, and constructed a collaborative application group. The newly proposed Hydra-Bite could resist the detecting and killing of multiple antivirus programs, which has higher information capture rate and stronger anti-killing performance. To achieve the isolation and access control for virtual machines and IoT devices, J. Dong et al. proposed a paper entitled "Task-Oriented Multilevel Cooperative Access Control Scheme for Environment with Virtualization and IoT." In the scheme, each user of the platform created tasks which could be divided into multiple levels to limit access between virtual machines and IoT terminals. Moreover, the network isolation, process isolation, and shared memory isolation could further enhance security for virtual machines and IoT terminals. The paper by B. Tang et al. entitled "Niffler: A Context-Aware and User-Independent Side-Channel Attack System for Password Inference," presented a novel side-channel attack system according to the user-independent features of tapping consecutive buttons to reconstruct the unlocking passwords on smartphones. Also, the Niffler used a Markov model to model the unlocking process and used the sequences with the highest probabilities as the attack candidates, which achieves high password guessing accuracy with only several attempts and few training samples. The paper by D. Wang et al., entitled "Resetting Your Password Is Vulnerable: A Security Study of Common SMS-Based Authentication in IoT Device," is aimed at gaining the control of IoT devices without firmware analysis. The fundamental idea was based on the observation that most of the official applications (call APP) had a common feature which is using an SMS authentication code sent to client phone to authenticate the client when he forgot his password for the APP. The author implemented a prototype tool to enable performing such brute-force SMS authentication code attack on IoT devices automatically.

4. System and Resource Optimization

The IoT and fog devices are typically deployed in resource (energy, computational, storage) constrained environments. The adoption of fog computing with IoT has a lot of optimization shortcomings such as network reliability optimization, energy balancing, and task allocation. Y. Li et al. in their paper, entitled "Reliable Ant Colony Routing Algorithm for Dual-Channel Mobile Ad Hoc Networks," presented reliable path under dual-channel condition (DSAR) system which contained a dual-channel communication model and a hierarchical network model to improve network bandwidth and to optimize the dual layer network, respectively. Also, the ant colony algorithm was used in the system for changes of network topology adaptability. To solve the IoT energy balancing problem, Y. Wang et al. in their paper, entitled "Gleer: A Novel Gini-Based Energy Balancing Scheme for Mobile Botnet Retopology," presented a novel Gini based energy balancing scheme (Gleer) for the atomic network as the basis of the heterogeneous multi-layer mobile botnet. The authors categorized atomic network into multiple groups with the dynamic energy threshold, estimated botnet energy gap, and regulated the probability for each node with the Gini coefficients to estimate in the Gleer which could significantly reduce user' detection awareness. For the task allocation problem in mobile devices, the paper by W. Zhu et al., entitled "Multitask Allocation To Heterogeneous Participants in Mobile Crowd Sensing", considered a multi-task allocation problem with the heterogeneity of participants (different participants with different devices and tasks). To solve the above problem, the authors proposed a greedy discrete particle swarm optimization with genetic algorithm operation by using heuristic strategies and the random two-point mutation/crossover operations in the genetic algorithm. Aiming to examine the relationship between places of interest and the spatial patterns of mobility flows, the paper by L. Huang et al., entitled "Mining the Relationship between Spatial Mobility Patterns and POIs", modelled a network with each partitioned region as a node and connected between them as links weighted by the mobility flows. The community detection algorithm and logistic regression method were adopted to discover spatial mobility patterns and achieved the classify spatial communities featured by places of interest, respectively. To conserve the energy and wireless communication bandwidth for IoT network, Q. Xu et al. proposed a paper entitled "Cluster-Based Arithmetic Coding for Data

Provenance Compression in Wireless Sensor Networks" and presented a new cluster based arithmetic coding method which could encode and decode the provenance in an incremental manner with a higher compression rate. Also, the authors used a mathematical function of the WSN's size to derive the optimal clustering size, which was greatly useful for IoT-Fog computing environment.

5. User Privacy Preservation and Data Protection

Protecting the user and data privacy is an essential topic in the traditional cloud-based scenario. However, it contains more challenge issues when meeting the distributed IoT-Fog environment. To improve the participation of sensing users and the authenticity of sensing data in the fog computing, J. Xiong et al. proposed a paper entitled "Achieving Incentive, Security, and Scalable Privacy Protection in Mobile Crowdsensing Services" constructing a privacy-preserving data aggregation scheme. The authors used the differential privacy mechanism and homomorphic encryption for protecting the sensing data which could ensure the privacy of the sensing users. Moreover, the authors gave a new auction game theory based secure multi-party auction mechanism to solve the problem of prisoners' dilemma incurred in the sensing data transaction. Aiming to promote quality of service and guarantee security and fairness for wireless sensor network (WSN) in IoT, Z. Lv et al. proposed a paper entitled "A Rational Exchange Protocol under Asymmetric Information in Wireless Sensor Networks." In the paper, the authors presented an entropy-based incentive model and used the model to design an entropy-based rational exchange protocol, which satisfied the correctness, security, fairness, and robustness, respectively. To improve the efficacy of fully homomorphic encryption (FHE) for IoT usage, the paper by W.-T. Song et al., entitled "Privacy Protection of IoT Based on Fully Homomorphic Encryption" improved the bootstrapping technique in the FHE scheme to accelerate the computation. The authors optimized the parameter range, generalized their ciphertext modulus, and introduced SIMD homomorphic computation techniques into the new proposed method to improve the efficiency. To protect the data embedded in electronics, sensors, and software against side-channel attack (like DPA) in IoT scenario, the paper by S. Zhang and W. Zhong entitled "A New Type of Countermeasure against DPA in Multi-Sbox of Block Cipher" gave a new type of a countermeasure scheme against DPA in multi-Sbox of block cipher by converting the multi-Sbox into permutations, reused permutation to turn it into a special reusable Sbox, and made these inputs of permutations random by masking. The new method could successfully prevent the attacker from accurately aligning the power consumption and guarantee the data privacy of the IoT devices.

6. Conclusions

The authors in the special issue highlight both the promise and the challenges faced by this emerging field of security and privacy challenges in IoT and fog computing. Their manuscripts identify the further related research for security and privacy issues in IoT-Fog scenario. Hopefully, the special issue serves as a remarkable source for graduate students, education, professors, researchers, and whoever interested in updating their knowledge of fog computing, IoT, and security and privacy issues for future information services and systems.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Ximeng Liu
Yang Yang
Kim-Kwang Raymond Choo
Huaqun Wang