Hindawi
Security and Communication Networks
Volume 2022, Article ID 9841709, 2 pages
https://doi.org/10.1155/2022/9841709

Editorial

Security, Trust and Privacy for Cloud, Fog and Internet of Things

Chien-Ming Chen,[1] **Shehzad Ashraf Chaudhry**,[2] **Kuo-Hui Yeh**,[3] **and Muhammad Naveed Aman**[4]

[1]*Shandong University of Science and Technology, Qingdao, China*
[2]*Istanbul Gelisim University, Istanbul, Turkey*
[3]*National Dong Hwa University, Hualien, Taiwan*
[4]*University of Nebraska-Lincoln, Lincoln, NE, USA*

Correspondence should be addressed to Chien-Ming Chen; chienmingchen@ieee.org

Received 5 January 2022; Accepted 5 January 2022; Published 28 January 2022

Internet of Things (IoT) is a promising networking scenario in the cyber world, bridging physical devices and virtual objects. By considering the limited capacity of smart things, cloud computing is generally applied to store and process the massive data collected by the IoT. Furthermore, fog computing is described as an extension and a complement to cloud computing. It utilizes fog nodes to perform storage, computation, and communication locally. The merging of cloud/fog computing and IoT can be seen as the best of two worlds by concurrently offering ubiquitous sensing services and powerful processing capabilities.

Despite the advantages of cloud/fog-assisted IoT, it is unwise to neglect the significance of security and privacy in this highly heterogeneous and interconnected system. Various solutions have recently been put forward independently for cloud, fog, or IoT environments to deal with security threats to IoT devices and sensitive data. However, a few crucial features, such as heterogeneity and scalability, have not been appropriately considered in these solutions.

This Special Issue aims to compile recent research efforts dedicated to studying the security and privacy of rapidly increasing cloud/fog-assisted IoT applications. A summary of all the accepted papers is provided as follows.

The paper by Mekala et al. designed a data analytic weight measurement (DAWM) model and multiobjective heuristic user service demand (MHUSD) approach for profit maximization and adequate service reliability. The DAWM model concentrates on instances or machine size with elastic service of generic lambda function to scale up and scale down the instance size as per demand request by considering instance computation status and its service execution rate and energy consumption. The MHUSD approach measures the CPS profit rate and USD rate before sharing the resources to the instances. The fundamental logic is if the instance DAWM rate is not above moderate or moderate, then the CSP does not share the resources as per demand; otherwise, the CSP shares the resources. In addition, the CSP scales up and down the cost of the resources as per the USD rate to maximize the profit (a business model).

In the paper by Zhang et al., a constant-size CP-ABE scheme with outsourced decryption for the cloud-assisted IoT is proposed. In their scheme, the ciphertexts and the attribute-based private keys for users are both of constant size, which can alleviate the transmission overhead and reduce the occupied storage space. And, the outsourced decryption algorithm in their work is privacy-protective, which means the proxy server cannot know anything about the access policy of the ciphertext and the attribute set of the user while performing the online partial decryption algorithm. This scheme can prevent privacy from leaking out to the proxy server. And, they have rigorously proved that their scheme is selectively indistinguishably secure under the chosen-ciphertext attacks (IND-CCAs) in the random oracle model (ROM). Finally, the authors evaluate and implement their scheme and other CP-ABE schemes in terms of space and time complexity to confirm that their scheme is more suitable and applicable for cloud-assisted IoT.

The paper by Pan et al. proposed an intrusion detection model. The model can be deployed in the architecture based on cloud computing and fog computing to play its role

better. The designed intrusion detection algorithm combines kNN and sine cosine algorithm (SCA). Specifically, SCA is used to optimize the hyperparameters of kNN, thereby improving the classification accuracy of kNN. This algorithm can significantly improve the accuracy of intrusion detection and reduce the false alarm rate. In the benchmark function test, the proposed algorithm shows good optimization efficiency.

In the paper by Wang et al., a bibliometric analysis of edge computing for the Internet of things was performed using the Web of Science (WoS) Core Collection dataset. The relevant literature published in this field was quantitatively analyzed based on a bibliometric analysis method combined with VOSviewer software. The development history, research hotspots, and future directions of this field were also studied. The research results show that the number of literature studies published in edge computing for the Internet of things is on the rise over time, especially after 2017, and the growth rate is accelerating.

The paper by Ullah et al. proposed a scheme named task priority-based data-prefetching scheduler (TPDS), which tries to improve the data locality through available cached and prefetching data for offloading tasks to the edge computing nodes. The proposed TPDS prioritizes the tasks in the queue based on the available cached data in the edge computing nodes. Consequently, it increases the utilization of cached data and reduces the overhead caused by data eviction. The simulation results show that the proposed TPDS can be effective in terms of task scheduling and data locality.

In the paper by Mahmood et al., a Software Defined Networking (SDN)-based DDoS Protection System named S-DPS is proposed. It provides an early detection mechanism with mitigation of anomaly in real time. The approach offers the best deployment location of defense mechanism due to the centralized control of the network. S-DPS has demonstrated its effectiveness and efficiency in terms of Detection Rate and minimal CPU/RAM utilization, considering DDoS protection focusing on smurf attacks, socket stress attacks, and SYN flood attacks.

The paper by Ling et al. proposed multiauthority attribute-based encryption with traceable and dynamic policy updating. The proposed T-DPU-MCP-ABE is used to protect user's data privacy and solve the problem that the single authorization center load is too large, the user key leakage cannot be traced, and the data owner frequently changes the access policy in cloud storage CP-ABE access control for IoT. The scheme is constructed on prime order groups over a large attribute universe. Therefore, it is more suitable for multiuser scenarios. The authors prove that the designed scheme is static, secure, and traceable based on state-of-the-art security models. Finally, through theoretical comparison and extensive experimental comparisons, the authors show that the proposed algorithm can be better than the baseline algorithms.

In the paper by Liao et al., a systematic literature review of the current solutions and approaches available for assessing the security of software components to protect software systems for the Internet of Things is presented. This paper searches the literature in the popular and well-known libraries, filters the relevant literature, organizes the filter papers, and extracts derivations from the selected studies based on different perspectives.

The paper by Tseng et al. proposed a generic construction of inner product predicate encryption under symmetric-key setting, called private inner product predicate encryption, from a specific key-homomorphic pseudorandom function. In addition, they show that the proposed construction is also payload-hiding, attribute-hiding, and predicate-hiding secure. With the advantage of the generic construction, if the underlying pseudorandom function can resist quantum attacks, then through the proposed generic construction, a quantum-resistant private inner product predicate encryption can be obtained. Hence, compared with other private inner product predicate encryption schemes, our scheme enjoys more robust security.

In the paper by Wu et al., a secure authentication and key agreement scheme is proposed. This scheme compensates for the imperfections of the previously proposed schemes. For a security evaluation of the proposed authentication scheme, informal security analysis, and the Burrows–Abadi–Needham (BAN) logic analysis are implemented. In addition, the ProVerif tool is used to normalize the security verification of the scheme. Finally, the performance comparisons with the former schemes show that the proposed scheme is more applicable and secure.

Conflicts of Interest

The Guest Editors declare that there are no conflicts of interest regarding the publication of the Special Issue.

Chien-Ming Chen
Shehzad Ashraf Chaudhry
Kuo-Hui Yeh
Muhammad Naveed Aman