Security and Privacy Issues of Fog Computing: A Survey

Shanhe Yi(✉), Zhengrui Qin, and Qun Li

College of William and Mary, Williamsburg, VA, USA
{syi,zhengrui,liqun}@cs.wm.edu

Abstract. Fog computing is a promising computing paradigm that extends cloud computing to the edge of networks. Similar to cloud computing but with distinct characteristics, fog computing faces new security and privacy challenges besides those inherited from cloud computing. In this paper, we have surveyed these challenges and corresponding solutions in a brief manner.

Keywords: Fog computing · Cloud/mobile computing · Security · Privacy

1 Introduction

The prevalence of ubiquitously connected smart devices are shaping the main factor of computing. Rapid development of wearable computing, smart metering, smart home/city, connected vehicles and large-scale wireless sensor network are making everything connected and smarter, termed the Internet of Things (IoT). IDC (International Data Corporation) has predicted that in the year of 2015, "the IoT will continue to rapidly expand the traditional IT industry" up 14 % from 2014 [14]. As we know, smart devices usually face challenges rooted from computation power, battery, storage and bandwidth, which in return hinder quality of services (QoS) and user experience. To alleviate the burden of limited resources on smart devices, cloud computing is considered as a promising computing paradigm, which can deliver services to end users in terms of infrastructure, platform and software, and supply applications with elastic resources at low cost.

Cloud computing, however, is not a "one-size-fit-all" solution. There are still problems unsolved since IoT applications usually require mobility support, geo-distribution, location-awareness and low latency. *Fog computing*, a.k.a edge computing, is proposed to enable computing directly at the edge of the network, which can deliver new applications and services for billions of connected devices [2]. Fog devices are usually set-top-boxes, access points, road side units, cellular base stations, etc. End devices, fog and cloud are forming a three layer hierarchical service delivery model, supporting a range of applications such as web content delivery [48], augmented reality [15], and big data analysis [46]. A typical conceptual architecture of fog/cloud infrastructure is shown in Fig. 1.

K. Xu and J. Zhu (Eds.): WASA 2015, LNCS 9204, pp. 685–695, 2015.
DOI: 10.1007/978-3-319-21837-3_67

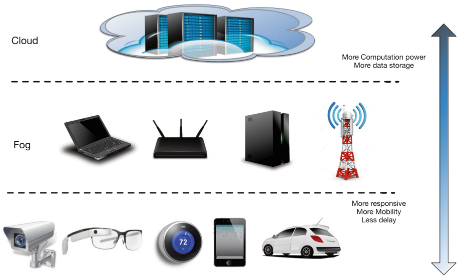

Fig. 1. An example of fog/cloud architecture

Since fog is deemed as a non-trivial extension of cloud, some security and privacy issues in the context of cloud computing [35], can be foreseen to unavoidably impact fog computing. Security and privacy issues will lag the promotion of fog computing if not well addressed, according to the fact that 74 % of IT Executives and Chief Information Officers reject cloud in term of the risks in security and privacy [49]. As fog computing is still in its infant stage, there is little work on security and privacy issues. Since fog computing is proposed in the context of Internet of Things (IoT), and originated from cloud computing, security and privacy issues of cloud are inherited in fog computing. While some issues can be addressed using existing schemes, there are other issues facing new challenges, due to the distinct characteristics of fog computing, such as heterogeneity in fog node and fog network, requirement of mobility support, massive scale geo-distributed nodes, location-awareness and low latency.

In this paper, we will discuss secur ity and privacy issues in fog computing by reviewing existing work of fog computing and related work in underlying domains, and identify new security and privacy problems.

2 Fog Computing Overview

In this section, we briefly give an overview of fog computing. We prefer not to discuss the cloud computing or mobile cloud computing, and readers can refer to extensive existing surveys if interested [8,47].

Definition. As a new paradigm of computing, fog computing is still not a full-fledged concept in the community. In the position paper [2], fog computing is considered as an extension of the cloud computing to the edge of the network, which is a highly virtualized platform of resource pool that provides computation, storage, and networking services to nearby end users. In the perspective of work [38], they have defined fog computing as "*a scenario where a huge number of heterogeneous (wireless and sometimes autonomous) ubiquitous and decentralised devices communicate and potentially cooperate among them and with the network to perform storage and processing tasks without the intervention of third parties. These tasks can be for supporting basic network functions or new services and applications that run in a sandboxed environment. Users leasing part of* *their devices to host these services get incentives for doing so.*" Although those definitions are still debatable before, fog computing is no longer a buzzword.

Characterization. Fog computing has its advantages due to its edge location, and therefore is able to support applications (e.g. gaming, augmented reality, real time video stream processing) with low latency requirements. This edge location can also provide rich network context information, such as local network condition, traffic statistics and client status information, which can be used by fog applications to offer context-aware optimization. Another interesting characteristic is the location-awareness; not only can the geo-distributed fog node infer its own location but also the fog node can track end user devices to support mobility, which may be a game changing factor for location-based services and applications. Furthermore, the interplays between fog and fog, fog and cloud become important since fog can easily gets local overview while the global coverage can only be achieved at a higher layer.

Fog Node. The ubiquity of smart devices and rapid development of standard virtualization and cloud technology make several fog node implementation available. *Resource-poor fog node* This kind of fog nodes is usually built on existing network devices. ParaDrop [42] is a new fog computing architecture on gateway (WiFi access point or home set-top box), which is an ideal fog node choice due to its capabilities to provide service and its proximity at network edge. Given the fact that typical home environment gateways are resource-limited, the authors implement the ParaDrop using Linux Container (LXC) abstraction which is more lightweight than traditional virtual machines. *Resource-rich fog node* Resource-rich fog nodes are usually specific high-end servers with powerful CPU, larger memory and storage. Cloudlet [29,30], like a "second-class data center", is able to provide elastic resources to nearby mobile devices, with low latency and large bandwidth. With cloud techniques, Cloudlet is easy to upgrade and replace.

Service Delivery and Deployment Models. Similar to cloud computing, we can anticipate that the service delivery models in fog computing can be grouped into three categories: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). We may also expect the following deployment models: private fog, community fog, public fog and hybrid fog.

Similar Concept. Mobile cloud computing (MCC) and mobile-edge computing (MEC) are similar to fog computing. MCC refers to an infrastructure in which both the data storage and the data processing happen outside of the mobile devices [8]. MEC focus on resource-rich fog servers like cloudlets running at the edge of mobile networks [11]. Fog computing distinguishes itself as a more generalized computing paradigm especially in the context of Internet of Things.

3 Security and Privacy Issues

We admit that security and privacy should be addressed in every layer in designing fog computing system. Here we ask ourselves "what is new about fog computing security and privacy?". Due to the characteristics of fog computing, we may need future work to tackle those problems.

3.1 Trust and Authentication

In cloud computing deployment, data centers are usually owned by cloud service providers. However, fog service providers can be different parties due to different deployment choices: (1) Internet service providers or wireless carriers, who have control of home gateways or cellular base stations, may build fog with their existing infrastructures; (2) Cloud service providers, who want to expand their cloud services to the edge of the network, may also build fog infrastructures; (3) End users, who own a local private cloud and want to reduce the cost of ownership, would like to turn the local private cloud into fog and lease spare resources on the local private cloud. This flexibility complicates the trust situation of fog.

Trust Model. Reputation based trust model [18] has been successful in eCommerce, peer-to-peer (P2P), user reviews and online social networks. Damiani et al. [7] proposed a robust reputation system for resource selection in P2P networks using a distributed polling algorithm to assess the reliability of a resource before downloading. In designing a fog computing reputation-based reputation system, we may need to tackle issues such as (1) how to achieve persistent, unique, and distinct identity, (2) how to treat intentional and accidental misbehavior, (3) how to conduct punishment and redemption of reputation. There are also trusting models based on special hardware such as Secure Element (SE), Trusted Execution Environment (TEE), or Trusted Platform Module (TPM), which can provide trust utility in fog computing applications.

Rogue Fog Node. A rogue fog node would be a fog device or fog instance that pretends to be legitimate and coaxes end users to connect to it. For example, in an insider attack, a fog administrator may be authorized to manage fog instances, but may instantiate a rogue fog instance rather than a legitimate one. Work [34] has demonstrated the feasibility of man-in-the-middle attack in fog computing, before which the gateway should be either compromised or replaced by a fake one. Once connected, the adversary can manipulate the incoming and outgoing requests from end users or cloud, collect or tamper user data stealthily, and easily launch further attacks. The existing of fake fog node will be a big threat to user data security and privacy. This problem is hard to address in fog computing due to several reasons (1) complex trust situation calls for different trust management schemes, (2) dynamic creating, deleting of virtual machine instance make it hard to maintain a blacklist of rogue nodes. Han et al. [16,17] have proposed a measurement-based method which enables a client to avoid connecting rogue access point (AP). Their approach leverages the round-trip time between end users and the DNS server to detect rogue AP at the client side.

Authentication. Authentication is an important issue for the security of fog computing since services are offered to massive-scale end users by front fog nodes. Stojmenovic et al. [34] have considered the main security issue of fog computing as the authentication at different levels of fog nodes. Traditional PKI-based authentication is not efficient and has poor scalability. Balfanz et al. [1] have proposed a cheap, secure and user-friendly solution to the authentication problem in local ad-hoc wireless network, relying on a physical contact for pre-authentication in a location-limited channel. Similarly, NFC can also be used to simplify the authentication procedure in the case of cloudlet [3]. As the emergence of biometric authentication in mobile computing and cloud computing, such as fingerprint authentication, face authentication, touch-based or keystroke-based authentication, etc., it will be beneficial to apply biometric-based authentication in fog computing.

3.2 Network Security

Due to the predominance of wireless in fog networking, wireless network security is big concern to fog networking. Example attacks are jamming attacks, sniffer attacks, etc. Those attacks can be addressed in the research domain of wireless network, which is not in the scope of this survey. Normally, in network, we have to trust the configurations manually generated by a network administrator and isolate network management traffic from regular data traffic [36]. However, fog nodes are deployed at the edge of Internet, which definitely bring heavy burden to the network management, imagining the cost of maintaining massive scale cloud servers which are distributed all over the network edge without easy access for maintenance. The employment of SDN can ease the implementation and management, and increase network scalability and reduce costs, in many aspects of fog computing. We also argue that applying SDN technique in fog computing will bring fog networking security new challenges and opportunities.

How can SDN help the fog network security? (1) Network Monitoring and Intrusion Detection System (IDS): CloudWatch [32] can leverage OpenFLow [21] to route traffic for security monitoring applications or IDS. (2) Traffic Isolation and Prioritization: Traffic isolation and prioritization can be used to prevent an attack from congesting the network or dominating shared resources such as CPU or disk I/O. SDN can easily use VLAN ID/tag to isolate traffic in VLAN group and segregate malicious traffic. (3) Network Resource Access Control: Klaedtke et al. [19] have proposed an access control scheme on a SDN controller based on OpenFlow, (4) Network Sharing: Fog-enhanced router in home network can be opened to guests, if the network sharing to guests is carefully designed with security concerns. Work [44] has proposed OpenWiFi, in which the guest WiFi authentication is shifted to the cloud to establish guest identity; access is independently provided for guests; and accounting is enforced to delegate responsibility of guests.

3.3 Secure Data Storage

In fog computing, user data is outsourced and user's control over data is handed over to fog node, which introduces same security threats as it is in cloud computing. First, it is hard to ensure data integrity, since the outsourced data could be lost or incorrectly modified. Second, the uploaded data could be abused by unauthorized parties for other interests.

To address these threats, auditable data storage service has been proposed in the context of cloud computing to protect the data. Techniques such as homomorphic encryption and searchable encryption are combined to provide integrity, confidentiality and verifiability for cloud storage system to allow a client to check its data stored on untrusted servers. Want et al. [40] have proposed privacy-preserving public auditing for data stored in cloud, which relies on a third-party auditor (TPA), using homomorphic authenticator and random mask technique to protect privacy against TPA. To ensure data storage reliability, prior storage systems use erasure codes or network coding to deal with data corruption detection and data repair, while Cao et al. [5] have proposed a scheme using LT code, which provides less storage cost, much faster data retrieval, and comparable communication cost. Yang et al. [43] have provided a good overview of existing work towards data storage auditing service in cloud computing.

In fog computing, there are new challenges in designing secure storage system to achieve low-latency, support dynamic operation and deal with interplay between fog and cloud.

3.4 Secure and Private Data Computation

Another important issue in fog computing is to achieve secure and privacy-preserving computation outsourced to fog nodes.

Verifiable Computing. Verifiable computing enables a computing device to offload the computation of a function to other perhaps untrusted servers, while maintaining verifiable results. The other servers evaluate the function and return the result with a proof that the computation of the function was carried out correctly. The term verifiable computing was formalized in [13]. In fog computing, to instill confidence in the computation offloaded to the fog node, the fog user should be able to verify the correctness of the computation.

Below are some existing methods to fulfill verifiable computing. Gennaro et al. [13] have proposed a verifiable computing protocol that allows the server to return a computationally-sound, non-interactive proof that can be verified by the client. The protocol can provide (at no additional cost) input and output privacy for the client such that the server does not learn any information about the input and output. Parno and Gentry have built a system, called *Pinocchio*, such that the client can verify general computations done by a server while relying only on cryptographic assumptions [25]. With Pinocchio, the client creates a public evaluation key to describe her computation, and the server then evaluates the computation and uses the evaluation key to produce a proof of correctness.

Data Search. To protect data privacy, sensitive data from end users have to be encrypted before outsourced to the fog node, making effective data utilization services challenging. One of the most important services is keyword search, i.e., keyword search among encrypted data files. Researchers have developed several searchable encryption schemes that allow a user to securely search over encrypted data through keywords without decryption. In [33], the authors proposed the first ever scheme for searches on encrypted data, which provides provable secrecy for encryption, query isolation, controlled searching, and support of hidden query. Later, many other schemes have been developed, such as [6,39].

3.5 Privacy

The leakage of private information, such as data, location or usage, are gaining attentions when end users are using services like cloud computing, wireless network, IoT. There are also challenges for preserving such privacy in fog computing, because fog nodes are in vicinity of end users and can collect more sensitive information than the remote cloud lying in the core network. Privacy-preserving techniques have been proposed in many scenarios including cloud [4], smart grid [28], wireless network [27], and online social network [24].

Data Privacy. In the fog network, privacy-preserving algorithms can be running in between the fog and cloud while those algorithms are usually resource-prohibited at the end devices. Fog node at the edge usually collects sensitive data generated by sensors and end devices. Techniques such as homomorphic encryption can be utilized to allow privacy-preserving aggregation at the local gateways without decryption [20]. *Differential privacy* [10] can be utilized to ensure non-disclosure of privacy of an arbitrary single entry in the data set in case of statistical queries,.

Usage Privacy. Another privacy issue is the usage pattern with which a fog client utilizes the fog services. For example in smart grid, the reading of the smart meter will disclose lots of information of a household, such as at what time there is no person at home, and at what time the TV is turned on, which absolutely breaches user's privacy. Although privacy-preserving mechanisms have been proposed in smart metering [22,28], they cannot be applied in fog computing directly, due to the lack of a trusted third party (i.e., a smart meter in smart grid) or no counterpart device like a battery. The fog node which can easily collect statistics of end user usage. One possible naive solution is that the fog client creates dummy tasks and offloads them to multiple fog nodes, hiding its real tasks among the dummy ones. However, this solution will increase the fog client's payment and waste resources and energy. Another solution would be designing a smart way of partitioning the application to make sure the offloaded resource usages do not disclose privacy information.

Location Privacy. In fog computing, the location privacy mainly refers to the location privacy of the fog clients. As a fog client usually offloads its tasks to the nearest fog node, the fog node, to whom the tasks are offloaded, can infer that the fog client is nearby and farther from other nodes. Furthermore, if a fog client utilizes multiple fog services at multiple locations, it may disclose its path trajectory to the fog nodes, assuming the fog nodes collude. As long as such a fog client is attached on a person or an important object, the location privacy of the person or the object is at risk.

If a fog client always strictly chooses its nearest fog server, the fog node can definitely knows that the fog client that is utilizing its computing resources is nearby. The only way to preserve the location privacy is through identity obfuscation such that even though the fog node knows a fog client is nearby it cannot identify the fog client. There are many methods for identity obfuscation; for example, in [41], the authors use a trusted third party to generate fake ID for each end user. In reality, a fog client does not necessarily choose the nearest fog node but chooses at will one of the fog nodes it can reach according some criteria, such as latency, reputation, load balance, etc. In this case, the fog node can only know the rough location of the fog client but cannot do so precisely. However, once the fog client utilizes computing resources from multiple fog nodes in an area, its location can boil down to a small region, since its location must be in the intersection of the multiple fog nodes' coverages. To preserve the location privacy in such scenario, one can utilize the method used in [12].

3.6 Access Control

Access control has been a reliable tool to ensure the security of the system and preserving of privacy of user. Traditional access control is usually addressed in a same trust domain. While due to the outsource nature of cloud computing, the access control in cloud computing is usually cryptographically implemented for outsourced data. Symmetric key based solution is not scalable in key management. Several public key based solutions are proposed trying to achieve fine-grained access control. Yu et al. [45] have proposed a fine-grained data access control scheme constructed on attribute-based encryption (ABE). Work [9] proposes a policy-based resource access control in fog computing, to support secure collaboration and interoperability between heterogeneous resources. In fog computing, how to design access control spanning client-fog-cloud, at the same time meet the designing goals and resource constraints will be challenging.

3.7 Intrusion Detection

Intrusion detection techniques are widely deployed in cloud system to mitigate attacks such as insider attack, flooding attack, port scanning, attacks on VM and hypervisor [23], or in smart grid system to monitor power meter measurements and detects abnormal measurements that could have been compromised by attackers [26,37]. In fog computing, IDS can be deployed on fog node system side to detect intrusive behavior by monitoring and analyzing log file, access control policies and user login information. They can also be deployed at the fog network side to detect malicious attacks such as denial-of-service (DoS), port scanning, etc. In fog computing, it provides new opportunities to investigate how fog computing can help with intrusion detection on both client side and the centralized cloud side. Work [31] has presented a cloudlet mesh based security framework which can detection intrusion to distance cloud, securing communication among mobile devices, cloudlet and cloud. There are also challenges such as implementing intrusion detection in geo-distributed, large-scale, high-mobility fog computing environ men to meet the low-latency requirement.

4 Conclusion

This paper discusses several security and privacy issues in the context of fog computing, which is a new computing paradigm to provide elastic resources at the edge of network to nearby end users. In the paper, we discuss security issues such as secure data storage, secure computation and network security. We also highlight privacy issues in data privacy, usage privacy, and location privacy, which may need new think to adapt new challenges and changes.

References

1. Balfanz, D., Smetters, D.K., Stewart, P., Wong, H.C.: Talking to strangers: authentication in ad-hoc wireless networks. In: NDSS (2002)
2. Bonomi, F., Milito, R., Zhu, J., Addepalli, S.: Fog computing and its role in the internet of things. In: Workshop on Mobile Cloud Computing. ACM (2012)
3. Bouzefrane, S., Mostefa, A.F.B., Houacine, F., Cagnon, H.: Cloudlets authentication in nfc-based mobile computing. In: MobileCloud. IEEE (2014)
4. Cao, N., Wang, C., Li, M., Ren, K., Lou, W.: Privacy-preserving multi-keyword ranked search over encrypted cloud data. TPDS **25**(1), 222–233 (2014)
5. Cao, N., Yu, S., Yang, Z., Lou, W., Hou, Y.T.: Lt codes-based secure and reliable cloud storage service. In: INFOCOM. IEEE (2012)
6. Cash, D., et al.: Dynamic searchable encryption in very-large databases: data structures and implementation. In: NDSS, vol. 14 (2014)
7. Damiani, E., et al.: A reputation-based approach for choosing reliable resources in peer-to-peer networks. In: CCS. ACM (2002)
8. Dinh, H.T., Lee, C., Niyato, D., Wang, P.: A survey of mobile cloud computing: architecture, applications, and approaches. WCMC **13**(18), 1587–1611 (2013)
9. Dsouza, C., Ahn, G.J., Taguinod, M.: Policy-driven security management for fog computing: preliminary framework and a case study. In: IRI. IEEE (2014)
10. Dwork, C.: Differential privacy. In: van Tilborg, H.C.A., Jajodia, S. (eds.) Encyclopedia of Cryptography and Security. LNCS, vol. 2011. Springer, Heidelberg (2011)
11. ETSI: Mobile-edge computing (2014). http://goo.gl/7NwTLE
12. Gao, Z., Zhu, H., Liu, Y., Li, M., Cao, Z.: Location privacy in database-driven cognitive radio networks: Attacks and countermeasures. In: INFOCOM. IEEE (2013)
13. Gennaro, R., Gentry, C., Parno, B.: Non-interactive verifiable computing: outsourcing computation to untrusted workers. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 465–482. Springer, Heidelberg (2010)
14. Gil Press: Idc: Top 10 technology predictions (2015). http://goo.gl/zFujnE
15. Ha, K., Chen, Z., Hu, W., Richter, W., Pillai, P., Satyanarayanan, M.: Towards wearable cognitive assistance. In: Mobisys. ACM (2014)
16. Han, H., Sheng, B., Tan, C.C., Li, Q., Lu, S.: A measurement based rogue ap detection scheme. In: INFOCOM. IEEE (2009)
17. Han, H., Sheng, B., Tan, C.C., Li, Q., Lu, S.: A timing-based scheme for rogue ap detection. TPDS **22**(11), 1912–1925 (2011)
18. Jøsang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. Decis. Support Syst. **43**(2), 618–644 (2007)
19. Klaedtke, F., Karame, G.O., Bifulco, R., Cui, H.: Access control for sdn controllers. In: HotSDN, vol. 14 (2014)

20. Lu, R., et al.: Eppa: an efficient and privacy-preserving aggregation scheme for secure smart grid communications. TPDS **23**(9), 1621–1631 (2012)
21. McKeown, N., et al.: Openflow: enabling innovation in campus networks. ACM SIGCOMM CCR **38**(2), 69–74 (2008)
22. McLaughlin, S., McDaniel, P., Aiello, W.: Protecting consumer privacy from electric load monitoring. In: CCS. ACM (2011)
23. Modi, C., et al.: A survey of intrusion detection techniques in cloud. J. Netw. Comput. Appl. **36**(1), 42–57 (2013)
24. Novak, E., Li, Q.: Near-pri: Private, proximity based location sharing. In: INFOCOM. IEEE (2014)
25. Parno, B., Howell, J., Gentry, C., Raykova, M.: Pinocchio: nearly practical verifiable computation. In: Security and Privacy. IEEE (2013)
26. Qin, Z., Li, Q., Chuah, M.C.: Defending against unidentifiable attacks in electric power grids. TPDS **24**(10), 1961–1971 (2013)
27. Qin, Z., Yi, S., Li, Q., Zamkov, D.: Preserving secondary users' privacy in cognitive radio networks. In: INFOCOM, 2014 Proceedings IEEE. IEEE (2014)
28. Rial, A., Danezis, G.: Privacy-preserving smart metering. In: Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society. ACM (2011)
29. Satyanarayanan, M., Bahl, P., Caceres, R., Davies, N.: The case for vm-based cloudlets in mobile computing. Perv. Comput. **8**(4), 14–23 (2009)
30. Satyanarayanan, M., et al.: An open ecosystem for mobile-cloud convergence. Commun. Mag. **53**(3), 63–70 (2015)
31. Shi, Y., Abhilash, S., Hwang, K.: Cloudlet mesh for securing mobile clouds from intrusions and network attacks. In: Mobile Cloud 2015)
32. Shin, S., Gu, G.: Cloudwatcher: network security monitoring using openflow in dynamic cloud networks. In: ICNP. IEEE (2012)
33. Song, D.X., Wagner, D., Perrig, A.: Practical techniques for searches on encrypted data. In: Security and Privacy. IEEE (2000)
34. Stojmenovic, I., Wen, S.: The fog computing paradigm: scenarios and security issues. In: FedCSIS. IEEE (2014)
35. Takabi, H., Joshi, J.B., Ahn, G.J.: Security and privacy challenges in cloud computing environments. IEEE Secur. Priv. **8**(6), 24–31 (2010)
36. Tsugawa, M., et al.: Cloud computing security: what changes with software-defined networking? In: Jajodia, S., Kant, K., Samarati, P., Singhal, A., Swarup, V., Wang, C. (eds.) Secure Cloud Computing. LNCS. Springer, Heidelberg (2014)
37. Valenzuela, J., Wang, J., Bissinger, N.: Real-time intrusion detection in power system operations. IEEE Trans. Pow. Syst. **28**(2), 1052–1062 (2013)
38. Vaquero, L.M., Rodero-Merino, L.: Finding your way in the fog: towards a comprehensive definition of fog computing. ACM SIGCOMM CCR **44**(5), 27–32 (2014)
39. Wang, C., Cao, N., Ren, K., Lou, W.: Enabling secure and efficient ranked keyword search over outsourced cloud data. TPDS **23**(8), 1467–1479 (2012)
40. Wang, C., Wang, Q., Ren, K., Lou, W.: Privacy-preserving public auditing for data storage security in cloud computing. In: INFOCOM. IEEE (2010)
41. Wei, W., Xu, F., Li, Q.: Mobishare: Flexible privacy-preserving location sharing in mobile online social networks. In: INFOCOM. IEEE (2012)
42. Willis, D.F., Dasgupta, A., Banerjee, S.: Paradrop: a multi-tenant platform for dynamically installed third party services on home gateways. In: SIGCOMM Workshop on Distributed Cloud Computing. ACM (2014)
43. Yang, K., Jia, X.: Data storage auditing service in cloud computing: challenges, methods and opportunities. World Wide Web **15**(4), 409–428 (2012)

44. Yap, K.K., et al.: Separating authentication, access and accounting: a case study with openwifi. Technical report, Open Networking Foundation (2011)
45. Yu, S., Wang, C., Ren, K., Lou, W.: Achieving secure, scalable, and fine-grained data access control in cloud computing. In: INFOCOM. IEEE (2010)
46. Zao, J.K., et al.: Pervasive brain monitoring and data sharing based on multi-tier distributed computing and linked data technology. Frontiers in Human Neuroscience 8 (2014)
47. Zhang, Q., Cheng, L., Boutaba, R.: Cloud computing: state-of-the-art and research challenges. J. Internet Serv. Appl. **1**(1), 7–18 (2010)
48. Zhu, J., et al.: Improving web sites performance using edge servers in fog computing architecture. In: SOSE. IEEE (2013)
49. Zissis, D., Lekkas, D.: Addressing cloud computing security issues. Future Gener. Comput. Syst. **28**(3), 583–592 (2012)