IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 7, 2017, accepted September 1, 2017, date of publication September 6, 2017, date of current version October 12, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2749422

Security and Privacy in Fog Computing: Challenges

MITHUN MUKHERJEE[1], (Member, IEEE), RAKESH MATAM[2], (Member, IEEE), LEI SHU[1,3], (Senior Member, IEEE), LEANDROS MAGLARAS[4], (Senior Member, IEEE), MOHAMED AMINE FERRAG[5,6], NIKUMANI CHOUDHURY[2], (Student Member, IEEE), AND VIKAS KUMAR[7], (Member, IEEE)

[1]Guangdong Provincial Key Laboratory of Petrochemical Equipment Fault Diagnosis, Guangdong University of Petrochemical Technology, Maoming 525000, China
[2]Computer Science and Engineering, IIIT Guwahati, Guwahati 781001, India
[3]School of Engineering, University of Lincoln, Lincoln LN6 7TS, U.K.
[4]School of Computer Science and Informatics, De Montfort University Leicester, Leicester LE1 9BH, U.K.
[5]Department of Computer Science, Guelma University, Guelma 24000, Algeria
[6]Networks and Systems Laboratory, Badji Mokhtar University, Annaba 23000, Algeria
[7]Bharat Sanchar Nigam Ltd., Patna 800001, India

Corresponding author: Lei Shu (lei.shu@ieee.org)

This work was supported in part by the Maoming Engineering Research Center of Industrial Internet of Things under Grant 517018 and in part by the National Natural Science Foundation of China under Grant 61401107.

ABSTRACT Fog computing paradigm extends the storage, networking, and computing facilities of the cloud computing toward the edge of the networks while offloading the cloud data centers and reducing service latency to the end users. However, the characteristics of fog computing arise new security and privacy challenges. The existing security and privacy measurements for cloud computing cannot be directly applied to the fog computing due to its features, such as mobility, heterogeneity, and large-scale geo-distribution. This paper provides an overview of existing security and privacy concerns, particularly for the fog computing. Afterward, this survey highlights ongoing research effort, open challenges, and research trends in privacy and security issues for fog computing.

INDEX TERMS Fog, fog computing, fog networking, security, privacy, IoT, privacy threats, security threats.

I. INTRODUCTION

Due to the significant physical distance between cloud service provider's Data Centers (DCs) [1] and End User (EU), cloud computing suffers from substantial end-to-end delay, traffic congestion, processing of huge amount of data, and communication cost. Although few companies like Apple are moving towards more environmental friendly 100 percent renewable DCs with the wind, solar, and geothermal energy, the carbon emission from DCs due to the round-the-clock operation will dominate on global carbon footprint. Fog computing emerges as an alternative to traditional cloud computing to support geographically distributed, latency sensitive, and Quality-of-Service (QoS)-aware Internet of Things (IoT) applications. *Fog computing* was first initiated by Cisco to extend the cloud computing to the edge of a network [2], [3]. Fog computing is a highly virtualized platform [4] that provides computing, storage, and networking services between EU and DC of the traditional cloud computing. Fog computing has the following characteristics [2]:

- Low latency and location awareness
- Supports geographic distribution
- End device mobility
- Capacity of processing high number of nodes
- Wireless access
- Real-time applications
- Heterogeneity

The OpenFog Consortium [5], a consortium of high-tech giant companies and academic institutions across the world, aims to standardize and promote fog computing in various fields. This consortium was founded by ARM, Cisco, Dell, Intel, Microsoft Corp., and the Princeton University Edge Laboratory on November 19, 2015. Most recently, OpenFog released its Reference Architecture (RA) [6] for fog computing on 13 February 2017. OpenFog Consortium workgroups are working towards creating an open architecture for fog computing to enable interoperability and scalability. Besides, fog computing is also supported by several companies such as Cloudlet [7] and Intelligent Edge by Intel [8].

Many technology enablers for fog computing in various fields discussed by Chiang and Zhang [9]. Some of the examples are EU experience by GE, TOYOTA, BMW, etc., network equipment like switches, gateway by Cisco, Huawei, Ericsson, etc. The current research trends reflect the tremendous potential of fog computing towards sustainable development in global IoT market.

A. CLOUD, FOG, AND EDGE COMPUTING

Fog Computing extends a substantial amount of data storage, computing, communication, and networking of cloud computing near to the end devices. Due to close integration with the front-end intelligence [10] enabled end devices, fog computing enhances the overall system efficiency, after that improving the performance of critical cyber-physical systems. An important key difference is that cloud computing tries to optimize resource in a global view, whereas fog computing organizes and manages the *local* virtual cluster.

Edge computing and fog computing terms are interchangeably used in both academia and industry. Although the main objectives of edge computing and fog computing are same, i.e., to reduce end-to-end delay and lower network congestion, however, they differ how they process and handle the data and where the intelligence and computing power are placed. The main idea of Edge computing [11], [12] is to push computation facility towards data sources, e.g., sensors, actuators, and mobile devices. In Edge computing, each individual edge component plays its role to process data locally rather than sending them towards the cloud, whereas, fog node decides whether to process the data from multiple data sources using its own resource or send to the cloud. Also, several services like Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and other cloud-related services are not supported in Edge computing, however, these services can be extended with fog computing.

To summary, Edge computing [11]–[13] is totally edge-localized, however, fog computing extends the computing and communication resources towards edge of the network.

B. THREE-TIER ARCHITECTURE

Fig. 1 illustrates the three-tier architecture [14], one of the basic and widely used architectures in fog computing. The tiers are discussed as follows:

- *Tier 1–Things/End Devices:* This tier consists of IoT-enabled devices including sensor nodes, EU's smart hand-held devices (e.g., smartphones, tablets, and smartwatches), and others. These end devices are often termed as Terminal Nodes (TNs). It is assumed that these TNs are equipped with Global Positioning System.
- *Tier 2–Fog:* This tier is also termed as fog computing layer. The fog nodes in this layer are comprised of network devices such as router, gateway, switch, and Access Points (APs). These fog nodes can collaboratively share storage and computing facilities.

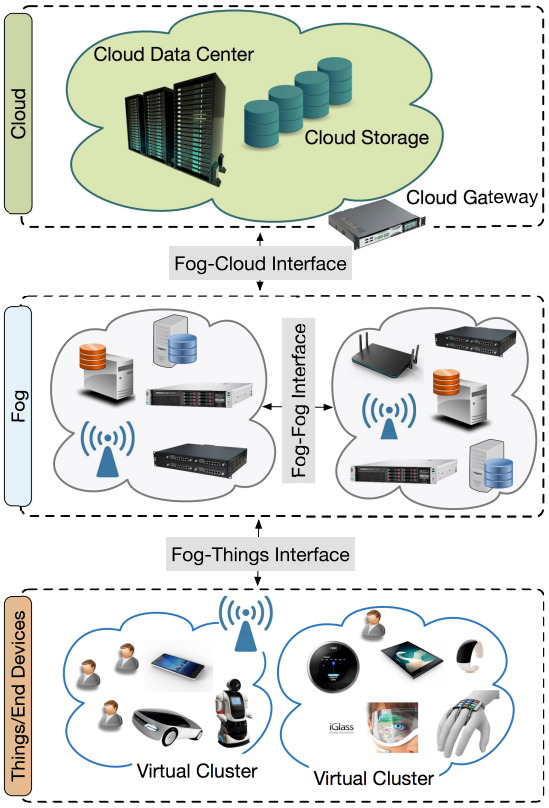


FIGURE 1. Three-tier fog computing architecture.

- *Tier 2–Cloud:* Traditional cloud servers and cloud DC reside in top-most tier. This tier has sufficient storage and computing resources.

A *fog-cloud interface* [9] is expected to provide end-to-end services including how the cloud will distribute service to the fog. In fog computing, several nodes or systems are scheduled to collaborate with each other to share data storage and computing tasks. Therefore, the design of fog-fog interface and protocol that enables different fog nodes to collaborate with each other is a significant challenge. In addition, *fog-thing interface* will securely enable efficient resource utilization.

C. RELATED SURVEYS AND OUR CONTRIBUTIONS

A brief overview of fog security and privacy issues is discussed in [15] and [16]. However, this survey is very limited regarding open research challenges in security and privacy issues for fog computing. Stojmenovic *et al.* [17], [18], discussed the security and privacy issues. Furthermore, some counter measurements are found in [19] and [20]. Recently, security and privacy preservation are discussed in fog-based vehicular networks [21]. Moreover, access authorization [22] and privacy-based query model for sustainable fog DCs [23] are discussed. While the aforementioned contributions [15], [16], [20], [24] have laid a solid foundation for the understanding of security and privacy issues in fog computing, this article differs from previous surveys in many aspects. For example, the work in [21] considers only vehicular-based crowdsensing, [24] focused on only fog forensics,

[20] discussed a brief overview of privacy and security. The above-mentioned study either *partially* considered the security and privacy issues or are in the *very* early stage. Moreover, an up-to-date summarization in these privacy and security aspects in fog computing is missing. The following summarizes our key contributions.

1) This article contributes with the key research challenges in fog security and privacy issues. In addition, this article provides a comprehensive survey on recent advancement towards secure and privacy-preserving fog computing.
2) Further, this study highlights the open research challenges and discusses the future research directions to overcome these challenges in fog computing.

The remainder of this article is organized as follows. The various issues in fog computing security and privacy are discussed in Section II. Section III provides an overview of state-of-the-art on fog computing security and privacy. The challenges and research issues in fog computing are addressed in Section IV. Finally, conclusions are drawn in Section V.

II. SECURITY AND PRIVACY ISSUES IN FOG COMPUTING

A. TRUST

IoT networks are expected to provide reliable and secure services to the EUs. This requires all devices that are part of the fog network to have a certain level of trust on one another. Authentication plays a major role in establishing initial set of relations between IoT devices and fog nodes in the network. But this is not sufficient as devices can always malfunction or are also susceptible to malicious attacks. In such a scenario, trust plays a major role in fostering relations based on previous interactions. Trust should play a two-way role in a fog network. That is, the fog nodes that offer services to IoT devices should be able to validate whether the devices requesting services are genuine. On the other hand, the IoT devices that send data and other valued processing requests should be able to verify whether the intended fog nodes are indeed secure. This requires a robust trust model in place to ensure reliability and security in fog network. Several works [25], [26] have been carried out to address the issue of trust in cloud computing environment. However, the unique challenges posed by fog computing environment necessitates to revisit this problem. Contrary to cloud computing environment, the need for a fog node to quantify past interactions with IoT devices in the form of trust/reputation is to be addressed.

Trust of a Fog Service: A potential EU in fog computing needs to ensure *trust-level* provided by the fog service providers. Therefore, it becomes necessary to answer:

- *How do we measure trust in a fog service and what are the main attributes that define the trust of the fog service?*

The well-established trust models in cloud computing can be directly applied to fog computing due to lack of centralized management and mobility issues. Even though fog service provider offers attributes to measure trust of a service, at the same time, following question will arise as

- *Who will verify and monitor these attributes?*

Among several trust-management model in cloud computing, reputation-based trust model is widely used in e-commerce services. Sometimes, reputation of a service provider is useful to choose among several service providers. As this service model strongly depends on overall opinion, it is not well well-suited in fog computing due to dynamic nature of EU devices and fog nodes in the fog layers. In addition, although, opinion-based model is helpful to choose a fog service, the reliability will become an important factor to be considered. Service Level Agreement (SLA) between a cloud service and EU has gained a significant attention in designing trust model in cloud computing. However, this SLA verification is limited when a user directly uses the cloud service, if the service is processed in the fog layer, a professional and licensed third-party should monitor SLA verification for the EUs and small organization who lack in technical capability.

B. AUTHENTICATION

Authentication of networked devices subscribed to fog services is one of the foremost requirement in fog network. To access the services of a fog network, a device has to first become part of the network by authenticating itself to the fog network. This is essential to prevent the entry of unauthorized nodes. It becomes a formidable challenges as the devices involved in the network are constrained in various ways including power, processing and storage. Traditional authentication mechanisms using certificates and Public-Key Infrastructure (PKI) are not suitable due to the resource constraints of IoT devices. Alternatively, authentication protocols like [27] have been proposed that is based on public-key infrastructure using multicast authentication for secure communications. In essence, like storage and processing services, authentication also needs to be offered as a service whereby a device that needs them would have to get authenticated to the fog node with the help of the intermediary that may be the Certifying Authority (CA). This model of operations would prevent unauthorized nodes from becoming part of the fog network. In addition, this would also allow the fog nodes to restrict service requests from malicious/compromised nodes.

Dynamic fog nodes and EUs: Similar to mobility issue in EUs, the fog nodes also frequently join and leave the fog layer. It is required to ensure the uninterrupted service to the registered end users when a new fog node joins (or leaves) the fog layer. The EU must be able to authenticate themselves to the newly formed fog layer mutually. From EUs perspective, the complexity of registration and re-authentication phase without huge overhead.

C. SECURE COMMUNICATIONS IN FOG COMPUTING

The way processing and storage requirements can be offloaded to fog nodes, security requirements cannot be offloaded. Even IoT devices need to implement the minimum security requirements. Communications between IoT devices

are considered to be taken care of the security practices in place for IoT communications. IoT devices interact with fog nodes only when they need to offload a processing or storage request. Any other interactions would not be considered as part of the fog environment as such communications would happen as part of the network. These fog nodes interact with each other when they need to effectively manage network resources or to manage network itself. They may even operate in distributed manner to perform a specific task. To secure communications in a fog computing environment the following communications between these devices are to be secured:

1) communications between constrained-IoT devices and fog nodes and
2) communications between fog nodes.

Usually, an IoT device can initiate communication with any of the fog nodes in the fog network requesting for a processing or storage requirement. In fact the IoT device may not even be aware of the existence of the fog network, therefore messages sent by such a device cannot be secured by using symmetric cryptographic techniques. Alternatively, asymmetric key cryptography has its set of challenges that are unique to IoT environment. Maintaining the PKI that is required to facilitate secure communication is one of the major challenge. Other challenges include minimizing the message overhead keeping in mind the constrained environment in which the IoT devices operate. Communications among fog nodes requires end-to-end security as nodes involved in multi-hop path may not be trust worthy.

D. END USER'S PRIVACY

Fog computing lies on the computational power of distributed nodes for reducing the total pressure of the data center. In fog computing, privacy preservation is more challenging since fog nodes that are in vicinity with EUs may collect sensitive data concerning the identity, usage of utilities, e.g. smart grid or location of end users compared to the remote cloud server that lies in the core network. Moreover, since fog nodes are scattered in large areas, centralized control is becoming difficult. The compromise of an poorly secured edge node can be the entry point for an intruder to the network. The intruder once inside the network can mine and steal users privacy data that is exchanged among entities. Increased communication among the three layers that constitute the fog architecture can also lead to privacy leakage. Location privacy, as discussed in [28], is one of the most important models for privacy, since the place of equipment can be linked to the owners. Since fog clients offload its tasks to nearest fog nodes, location, trajectory and even mobility habits can be revealed from an adversary. User habits can also be revealed from an adversary by analyzing his/her usage habits of fog services, e.g. smart grid. As shown in [29] smart meters' readings can disclose information about the time that the house is empty or even the TV programs that the EU prefers to watch.

As new systems that are based on fog computing are proposed, new privacy challenges also arise. Ni *et al.* [21] propose the idea of Fog-based Vehicular CrowdSensing (FVCS). In this system vehicular fog nodes can temporarily store and analyze all sensing data, that is uploaded by vehicles, in order to provide local services, taking the role of central cloud servers. By exchanging data about local situation, e.g. traffic jam, each car can help in optimizing several parameters of the vehicle network, exposing on the same time sensitive data about their owners regarding their location, trajectory etc. The anonymization of the information and the tasks of different entities that need to be done for each task could put a heavy burden on pseudonym management for both customers and the cloud [21].

Even if systems are well designed and securely implemented, they can expose critical information through their side channels. Possibilities of information leakage via side channels are pointed out in the literature and include electromagnetic radiation, observably timing of certain activities, power consumption of certain devices and even light acoustic or heat emanations from equipment [30]. All these privacy issues arise the need for more sophisticated solutions and countermeasures. Existing recent works are presented in the following sections.

E. MALICIOUS ATTACKS

Fog computing environment can be subjected to several malicious attacks and without proper security measures in place may severely undermine the capabilities of the network. One such malicious attack that can be launched is a Denial-of-Service (DoS) attack. Since majority of the devices connected to the networks are not mutually authenticated, launching a DoS attack becomes straight forward. The attack may be launched when devices that are connected to IoT network request for infinite processing/storage services. That is a compromised or malfunctioning node can make repeated processing/storage requests to a fog node thereby stalling requests made by legitimate devices. The intensity of such an attack rises manifold when a set of nodes simultaneously launch this attack. Another way to launch this attack is to spoof addresses of multiple devices and send fake processing/storage requests. Existing defense strategies of other types of networks are not suited for fog computing environment mainly due to the openness of the network. The first major challenge is the size of the network. Potentially, hundreds and thousands of nodes forming an IoT network avail the services of fog/cloud to overcome computation and storage limitations and also enhance performance. Since all these devices cannot be authenticated by fog nodes, they may rely on trusted third party like a certification authority that issues some form of credentials to ensure device authentication. But, the existence of such credentials only allows the processing fog node to verify whether the request has been generated by a legitimate node. Since a compromised node is a legitimate part of the network, all such requests would be entertained. On the other hand, restricting connectivity to the network or filtering the requests made by IoT devices nullifies the motivation of existence of fog nodes. Spoofing of addresses is also relatively easier as the address space is

relatively large and lack of boundaries makes it even more difficult.

Malicious Insider to the cloud: One of the severe attacks to the cloud computing is the data theft attack by a malicious insider to the cloud provider. Basically, the end users have to trust on cloud service provider. Thus, lack of cloud providers authentication results in data theft. Many incidents such as Twitter's personal and corporate data hacking [37], [38] and U.S. President Barack Obama's account hacking [39] reveal that the end user's password can be stolen effortlessly by a malicious insider. Rocha and Correia [40] discussed that the malicious insider to a cloud can easily get access to the user data, however, end-users do not detect the unauthorized access since the attack came from cloud service provider inside.

Although many approaches are useful to secure data in cloud computing using encryption and access control, misconfigured service, faulty implementation, bugs in code restrict them to fully protect from sophisticated attacks [41]. User behavior profiling can be useful to monitor the amount and duration of user data access. It can helps to detect the abnormal behavior of end-user, which can be further used to predict the malicious attacks. Recently, Stolfo *et al.* [31] proposed a new level of security for the cloud. Based on the user behavior profiling, if the abnormal behaviour is detected, then the decoy information is delivered to the true uses to obtain the response by many ways, e.g., security challenges. Otherwise, the decoy delivers a massive amount of garbage data to the attackers, thereafter, reducing the stolen information of the users. At the same time following issues arise as:

- Where to *place the decoy* in fog networks?
- How to design *on-demand decoy information* to further reduce the amount of stolen data.

III. EXISTING RESEARCH IN FOG COMPUTING SECURITY AND PRIVACY

Table 1 summarizes the state-of-the-art and research challenges in security and privacy issues for fog computing.

A. FOG NETWORK SCALABILITY

The EU mobility, one of the main characteristics of fog computing, introduces many security and privacy issues in fog network. Moreover, fog nodes are very dynamic in nature as fog nodes join or leave the fog layer very frequently. The well-studied approaches in cloud computing are not directly applied due to several reasons. For example, although the traditional PKI-based authentication is studied in [17], this approach is not suitable to implement at the massive scale of fog node and EUs. Furthermore, password-based authentication [52]–[54] is well-studied in cloud computing, however, it has many drawbacks as follows: 1) EUs are resource constraint, thus, extensive computation restricts the further implementation at EU level and 2) since, the fog nodes usually collaborate among themselves, one common password does not provide high security due to many attacks [55], such as vulnerability to off-line dictionary attack. Furthermore, the authentication scheme based on Diffie-Hellman [56] key exchange is not worthy due to slow and extensive modulo computations.

To address some of the above limitations, Ibrahim [32] proposed an efficient and secure authentication scheme that allows any EU to authenticate with any fog Node mutually. Using this scheme, the randomly roaming EU authenticates with any fog node that joins (or leaves) the fog layer very frequently, without a significant increase of overload. This feature makes the scheme suitable for resource-constraint EUs devices. The fog node (say, servers) in the fog layer are required to store only one secret key for each EU. The EU stores the only one long-lived master secret key in the registration phase. Using, this key, the EU mutually authenticates with any fog node managed by the cloud service provider. Since a few hash invocations and symmetric key encryption and decryption are required, it is suitable for a massive number of fog nodes and EUs without any PKI.

B. AUTHENTICATION AND PRIVACY-PRESERVING SCHEMES FOR FOG COMPUTING

Table 2 summarizes the authentication and privacy-preserving schemes for fog computing. Hu *et al.* [42] proposed three schemes, namely, 1) identity authentication scheme, 2) data encryption scheme, and 3) data integrity checking scheme, for fog computing with face identification and resolution application. Based on three main countermeasures, including, authentication and session key agreement, Advanced Encryption Standard (AES) symmetric key encryption mechanism based on session key, and Secure Hash Algorithm-1 (SHA-1), these three schemes can provide confidentiality, integrity, and availability under fog computing in IoT. Using Chinese remainder theorem, Lu *et al.* [43] introduced a Lightweight Privacy-preserving Data Aggregation (LPDA) scheme, for fog computing-enhanced IoT. The LPDA can aggregate hybrid IoT devices' data into one, as well as can resist against the false data injection attack. In addition, the LPDA scheme is efficient in term of computational costs and communication overhead compared to the aggregation with the basic Paillier encryption, but the traceability is not considered. Wang *et al.* [48] introduced a differential privacy-based query model for sustainable fog computing supported data center. Using Laplacian mechanism, this query model is efficient in terms of execution efficiency, privacy preserving quality, data utility, and energy consumption compared with traditional privacy preserving models. To solve the privacy preserving issue for the proximity detection in a fog computing system, Huo *et al.* [49] proposed a Location Difference-based Proximity Detection (LoDPD) protocol. Specifically, the LoDPD protocol uses the Paillier encryption algorithm and decision-tree theory in order which can protect the privacy of the users' location from disclosing to any party. Compared with the Private Proximity Detection (PPD) protocol [50], the LoDPD protocol is efficient in term of the communication cost.

TABLE 1. Summary of state-of-the-art and research challenges.

Challenges	Description	Focus/Objective	Contribution	Research opportunities
Malicious or Malfunctioning fog nodes.	A malicious or malfunctioning fog node can be source of data breach.	How to safeguard data against such attacks.	An efficient end-to-end security and encrypted data storage scheme that allows only IoT devices to store and access.	• The choice of encryption or proxy-encryption is a challenge in view of power complexities of IoT devices. • Design/adaptation of a low-cost end-to-end security scheme
Malicious insider attack [31]	Malicious attacker steals the EU's private key and illegitimately accesses the user data.	How to identify the malicious insider and reduce the amount of stolen information.	Based on the user behavior profiliation decoy technology is deployed using fog computing The decoy information return a massive amount of garbage data which is assumed to be true user's data to the attacker.	• Where to place the decoy in fog networks? • How to design on-demand decoy information to further reduce the amount of stolen data.
Mutual authentication among dynamic fog node and EUs [32]	The EUs roam randomly over the network. Besides, a fog nodes also frequently join and leave the fog layer. Thus, the mutual authentication EU and fog node is challenging issue.	How the EU is able to mutually authenticate with new fog node that joins the network without any significant increase in overheads.	• An efficient and secure authentication scheme that allows any EU and any fog node to authenticate each other. • The EU stores the only one long-lived master secret key, by which the EU mutually authenticates with any fog node managed by the cloud service provider.	How to keep the anonymity of the users and to trace the users with their true identity once user misbehave is detected by the cloud service provider.
Privacy preservation for UAV-assisted fog computing [33]	UAVs become a part of the fog computing and can be accessed ubiquitously. Moreover, this topological structures can be exploited by the attacker.	• How to provide the location privacy for UAVs-assisted fog computing? • How to guarantee the identity privacy for UAVs-assisted fog computing?	• An effective strategy for location privacy based on pseudonym changing. • A group signature based technique for achieving conditional location privacy without pseudonyms changing.	• How to integrate UAVs into the fog computing? • How to design a privacy-preserving scheme that reduces the costs in terms of storage cost, computation complexity, communication overhead and delay overhead?
Fog forensics [24]	Provides the digital evidence by reconstructing the past fog computing events.	How the retrieve log data from a large number of fog nodes?	Identifies the characteristics of fog forensics and how they are different from centralized cloud forensics.	• Require international legislation and jurisdictions [34], [35] • cross-border legislation challenges in fog computing.
Authentication and Key Agreement in F-RAN [36]	F-RAN is vulnerable to network attacks, such as replay attack, man-in-the-middle attack, and DoS attack.	• How to achieve scalable, authentication and billing in the context of F-RANs ? • How to achieve the client-to-server authentication, the server-to-client authentication and key agreement under the random oracle model?	• An authentication and key agreement protocol based on public key cryptosystem. • A privacy-preserving authentication scheme based on elliptic curve cryptography. • A unified auxiliary channel authentication protocol.	• How to design an authentication and key agreement protocol for F-RANs using software-defined networking (SDN) and network functions virtualization (NFV) technologies? • How to model the replay attack, man-in-the-middle attack, and DoS attack in F-RANs?

Supporting fine-grained access control in a fog storage system can be considered as an important issue, as discussed in the work [30], where Koo and Hur proposed a deduplication scheme for encrypted data. Using user-level key management and update mechanisms, the scheme [30] can support fine-grained access control in a fog storage system. Compared to the scheme [46], the scheme [30] is efficient in terms of computation, communication, and storage, but the adversary model is limited. However, the uses of the fog computing paradigm can improve the effectiveness of certificate revocation distribution in IoT environments, as discussed in the work [20], where the authors proposed a scheme based on the four system entities, including, a CA, a back-end cloud, fog nodes, and IoT devices. In the bounded retrieval model, Yang *et al.* [47] proposed a secure positioning protocol with location privacy for location-based fog computing. Xiao *et al.* [22] introduced a hybrid solution for fine-grained owner-enforced search in fog computing environment. Specifically, the scheme [22] is based on three main phases, including,1) System initialization, 2) Sensitive data outsourcing storage, and 3) Search and access of outsourced sensitive data.

Fog-based vehicular crowdsensing is an emerging paradigm, as discussed by Ni *et al.* [21]. However, authentication and privacy-preserving are critical aspect related to the functionality of crowdsensing reports. Basudan *et al.* [44]

TABLE 2. Summary of authentication and privacy-preserving schemes for fog computing.

Scheme	System Model	Authentication and privacy models	Countermeasure	Performances (+) and limitations (-)
Hu et al. [42]	fog computing with face identification and resolution application	• Confidentiality; • Integrity; • Availability.	• Authentication and session key agreement; • AES symmetric key encryption mechanism based on session key; • SHA-1 algorithm.	+ Response time for different face databases; + Amount of network transmission from fog nodes to cloud server; + Can detect man-in-the-middle attack and identity forgery; - Increases a little computation and communication overhead.
Lu et al. [43]	Fog computing-enhanced IoT	• Privacy of individual IoT device data; • Integrity.	• Chinese remainder theorem; • Homomorphic Paillier encryption; • One-way hash Chain.	+ Computational cost and communication overhead compared to the aggregation with the basic Paillier encryption; + Can resist against the false data injection attack; + Fault-Tolerance; - Traceability is not considered.
Basudan et al. [44]	Vehicular crowdsensing using fog computing	• Confidentiality; • Mutual authenticity; • Integrity; • Privacy; • Anonymity.	• Certificateless aggregate signcryption	+ Computational cost and communication overhead; + Key escrow resilience; + Provide anonymity compared to the scheme [42]; - Location privacy is not considered compared to the scheme [45].
Koo and Hur [30]	Fog storage architecture with the three system entities, including the cloud, fog, and end user	• Data privacy; • Forward secrecy.	• Pairing-based cryptographic; • Merkle tree; • User-level key management and update mechanisms.	+ Secure user-level key management; + Efficient in terms of computation, communication, and storage compared to the scheme [46]; - Adversary's model is limited.
Liu et al. [45]	VANET using fog computing	• Identity privacy; • Location privacy; • Authenticity.	• Location based encryption (LBE) scheme; • Cryptographic puzzle; - SHA-1 algorithm.	+ Average delay to solve a puzzle; + Average delay to verify the proofs; + Defending denial-of-service attacks; - Anonymity is not considered compared to the scheme [44]; - Adversary's model is limited.
Yang et al. [47]	Location-based fog computing	• Location privacy	• Position based cryptography (e.g., position based key exchange, • position based multi-party computation, position based public key infrastructure)	+ Without introducing additional computation overhead; - Integrity is not considered.
Xiao et al. [22]	Fog computing environment with four entities, including, data owner, cloud server, fog node, and many users	• Keyword privacy; • Data confidentiality; • Trapdoor unlinkability.	• Online/offline ABE technique; • Secure index generation; • Searchable encryption.	+ Swapping attack resistance; + Asymptotic complexity and actual implementation efficiency; + Resist swapping attack; + Secure against chosen keyword attack; - The perfect forward and backward secrecy are not considered.
Du et al. [23]	Fog data center consists with 4 renewable fog nodes	• Differential privacy	• Query function; • Laplacian mechanism.	+ Efficient in terms of execution efficiency, privacy preserving quality, data utility, and energy consumption; + Resist node and edge recognition attack; - Adversary's model is limited.
Wang et al. [48]	Fog computing with three parts, including, users, the fog server, and the location-based service (LBS) server	• Trajectory privacy; • Anonymity.	• Dummy rotation algorithm	+ Can achieve enhanced privacy preservation; - Integrity is not considered compared to the scheme [43].
Huo et al. [49]	A cloud network with three types of entities of fog network, including Alice, her friend Bob and a fog server of the service provider.	• Location privacy	• Paillier encryption algorithm; • Decision-tree theory.	+ Efficient in term of the communication cost compared with the PPD protocol proposed in [50]; - Traceability is not considered.
Wang et al. [51]	Fog-based public cloud computing with four types of entities, including, system manager, terminal devices, a fog node, and a public cloud server.	• Anonymity; • Identity privacy.	• Elliptic curve public-key cryptography; • Castagnos-Laguillaumie cryptosystem.	+ Efficient in terms of computation and communication; - Adversary's model is limited; - Location privacy is not considered.

proposed a privacy-preserving scheme, called Certificate Less Aggregate SignCryption scheme (CLASC), for vehicular crowdsensing using fog computing. The CLASC scheme can achieve data confidentiality, integrity, mutual authentication, privacy, and anonymity. In addition, the CLASC scheme has the lowest computational cost compared to the

existing schemes, but the location privacy is not considered. Similarly to the work [44], Liu *et al.* [45] introduced two secure traffic light control schemes in Vehicular Ad hoc NETwork (VANET) using fog computing. Based on two countermeasures, namely, 1) Location based encryption and 2) cryptographic puzzle, these two schemes are efficient to defending denial-of-service attacks, but the anonymity is not considered compared to the scheme [44] and adversary's model is limited. Wang et al. [48] proposed a Dummy Rotation (DR) algorithm to ensure the anonymity on a fog structure for cloud location services. The DR algorithm can achieve privacy-preserving by four privacy metrics, namely, 1) trajectory disclosure probability, 2) position disclosure probability, 3) average Euclidean distance, and 4) local data volume. Similarly to the scheme [43], Wang *et al.* [51] proposed an aggregation scheme in fog-based public cloud computing, called anonymous and secure aggregation scheme (ASAS). Specifically, the ASAS scheme considers a fog-based public cloud computing with four types of entities, including, system manager, terminal devices, a fog node, and a public cloud server. Based on two main countermeasures, namely, 1) Elliptic curve public-key cryptography and 2) Castagnos Laguillaumie cryptosystem, the ASAS can preserve the anonymity and identity privacy, but the adversary's model is limited.

C. FOG FORENSICS

The cloud forensic [57] provides the digital evidence by reconstructing past cloud computing events. Basically, it has the challenges in three dimensions as follows [57]: 1) *technical dimension* includes the inaccessibility to obtain *log data* from the cloud, volatile data, integrity and correctness of the data, and multi-tenancy, 2) *organizational dimension* refers to lack of forensics experts, in addition, 3) *legal dimension* focuses on customer awareness, Internet regulation, and cross-border law. Few steps are already taken to overcome some of these above issues. For example, Biggs and Vidalis [34] and Wolthusen [35] considered global unity to overcome the cross-border issue. Moreover, a continuous synchronization [58] was suggested to handle volatile data. Furthermore, the isolation of cloud instances [59] is proposed to overcome the multi-tenancy issues.

Followed by cloud forensic, fog forensic is defined as the application of digital forensics in fog computing. As observed by Wang *et al.* [24], fog forensics that have some steps similar to cloud forensic, however, is not a part of cloud forensics. Although some challenges in fog forensics are same as cloud forensics (e.g., cyber-physical systems and custody chain dependency, and integrity preservation), many challenges are more significant in fog forensics compared to cloud forensics. For example, since fog computing consists of massive number of fog nodes as infrastructure, retrieving the *log data* from these fog nodes becomes very difficult. Nevertheless, fog computing is geographically distributed, thus the cross-border issue is less critical compared to the centralized cloud forensics. However, due to a large number of fog nodes, the dependability issue becomes more crucial in fog forensics.

IV. OPEN QUESTIONS AND RESEARCH CHALLENGES

The cloud computing is generally heavily protected by cloud operators, nevertheless, all of the security solutions cannot be easily extended to fog computing due to many reasons. Although a few works, such as [16], [21], [30], [48], [60]–[62], considered the secure interaction of fog elements, authentication, and authorization for the fog computing, intruder detection, key agreements for fog computing, these approaches are either partially addressed the security and privacy issues or still in very early stages. This section outlines the open research challenges in fog security and privacy issues. Fig. 2 illustrates some of the open research challenges in fog privacy and security issues.

A. TRUST

Addressing issues related to trust in a fog network is slightly trickier compared to cloud computing environment. The openness of fog computing environment and the two-way requirement of trust are major challenges in designing a trust model for fog network. In other words, cloud computing environment have an in place security infrastructure adhering to security standards of the industry that allows EUs and businesses to develop a level of trust over the cloud. On the other hand, this is absent in FogNet that makes it more open and vulnerable to security attacks. Even though a common security framework can be employed by all the fog nodes forming the FogNet, high dynamism makes it challenging in addressing the issue of trust. In addition, trust is two-way requirement in FogNet but it is more-or-less unidirectional in cloud computing. Businesses and end users subscribing to cloud can quantify trust relationships and any malicious activity of end users can be defended using firewalls, intrusion detection systems and other security practices.But, in a FogNet the fog nodes also need to maintain trust relations with the devices using fog network services. Also, the IoT devices that entrust fog nodes with data and processing requests need to develop trusted interactions with the fog nodes. This two-way challenge in FogNet makes the design of trust model a formidable challenge.

B. PRIVACY PRESERVATION

As resources of EU's devices are shared among other *geographically* close devices to support context-aware services [63], [64], location, massive amount data and other information of EU need to be protected in very secure manner. As an use-case scenario, in [33], where a Unmanned Aerial Vehicles (UAVs)-based integrative IoT platform for integrating UAVs into the fog computing is suggested, the attackers through communication attacks such as the Man-In-The-Middle (MITM) attack easily exploit this platform to disclose sensitive information such as location and identity of the fog nodes. Therefore,

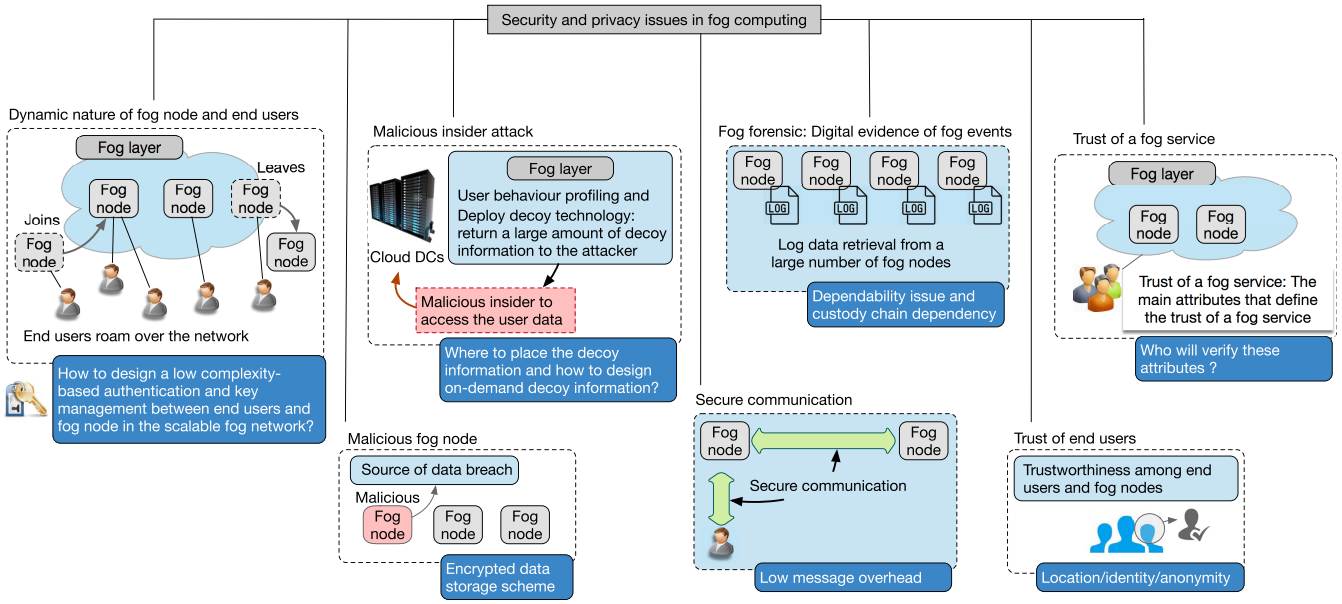


FIGURE 2. Open research challenges in fog security and privacy issues.

- how to provide the *location and identity privacy for fog computing* is challenging issue.

C. AUTHENTICATION AND KEY AGREEMENT

Authentication at different level of gateways is one of the major concern in fog computing where fog nodes are acting as data aggregation and control point of data collected from resource-constraint devices. Thus, a light-weight as well as end-to-end authentication is equally important in this context. For example, in fog computing-based radio access networks (F-RANs) [36], which is adaptive to the dynamic traffic and radio environment, how to achieve scalable, authentication and billing in the context of F-RANs is one of the most important issues. Hence,

- the authentication and key agreement protocols for F-RANs are major challenges and should be exploited in the future.
- In addition, user-level key management and update mechanisms to support fine-grained access control in a fog storage system is an important task.

D. INTRUSION DETECTION SYSTEMS

Intrusion Detection methods are widely used nowadays in order to mitigate attacks such as scanning attacks, dos attacks, insider attacks or MITM attacks and can be applied to different systems, e.g. SCADA [65], cloud [66], smart grid [67] etc. In fog computing IDS must be deployed in a all the levels of the three tier architecture monitoring and analyzing traffic and behavior of fog nodes, end devices and cloud servers. Securing one level of the system is not enough to guarantee that a virus or malware will not propagate from a vulnerable node to the rest of the system. By deploying IDS mechanisms to each level of a fog computing, challenges like real time notification, alarm parallelization, false alarm control and correct response arise [68]. A deployment of a perimeter Intrusion Detection System that can coordinate the different detection components that will be spread inside the fog system is needed [69].

E. DYNAMIC JOIN AND LEAVE OF FOG NODE

Since the fog node leaves or joins a fog layer very frequently, critical security issues arise as follows:

- How to handle the security and privacy issues when a *Fog node joins or leaves the fog layer*? For example, how the EUs authenticate themselves to the *new* fog node and how the privacy of the EUs can be preserved when a *Fog node leaves the fog layer*?
- How to design a *low complexity-based* authentication between EU and fog node in the *scalable* fog network?
- How to keep the *anonymity* of the users and to trace the users with their *true* identity once user misbehavior is detected by the cloud service provider?

F. CROSS-BORDER ISSUE AND FOG FORENSIC

Although the cross-border issue is less significant as compared to cloud computing due to distributed nature of fog computing, the fog forensics still require international legislation and jurisdictions [34], [35] and application level logging [70]. Therefore, it is still an important task to overcome cross-border legislation challenges in fog computing.

V. CONCLUSION

Security and privacy issues are well-studied in cloud computing, however, all of them are not suitable for fog computing due to several distinct characteristics of fog computing as well as a wider scale of fog devices at the edge of the network.

In addition, many new security and privacy threats arise that were not present in centrally-managed cloud computing. In this article, we have presented an overview of main security and privacy issues in fog computing. Afterward, this article surveys the state-of-the-art to deal with the fog computing-related security and privacy challenges. In summary, the aim of this survey is to summarize up-to-date research contributions and to outline future research direction to solve different challenges in privacy and security in the fog computing.

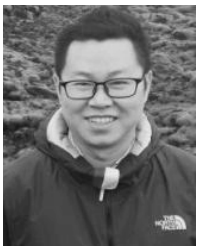
REFERENCES

[1] *Data Center Companies*. Accessed: Jul. 23, 2017. [Online]. Available: https://www.datacenters.com/directory/companies
[2] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. 1st Ed. MCC Workshop Mobile Cloud Comput. (MCC)*, Helsinki, Finland, Feb. 2012, pp. 13–16.
[3] Cisco. *Cisco Delivers Vision of Fog Computing to Accelerate Value from Billions of Connected Devices. Press Release*. Accessed: Jul. 23, 2017. [Online]. Available: https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1334100
[4] M. Aazam and E. N. Huh, "Fog computing: The cloud-IoT/IoE middleware paradigm," *IEEE Potentials*, vol. 35, no. 3, pp. 40–44, May 2016.
[5] *OpenFog Consortium*. Accessed: Jul. 23, 2017. [Online]. Available: https://www.openfogconsortium.org
[6] *OpenFog Reference Architecture*. Accessed: Jul. 23, 2017. [Online]. Available: https://www.openfogconsortium.org/ra/
[7] *Akami Cloudlet Overview*. Accessed: Feb. 20, 2017. [Online]. Available: https://www.akamai.com/us/en/products/web-performance/cloudlets/
[8] *Intelligent Edge Intel*. Accessed: Feb. 20, 2017. [Online]. Available: https://itpeernetwork.intel.com/extending-intelligence-to-the-edge/
[9] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 1–11, Dec. 2016.
[10] A. Bader, H. Ghazzai, A. Kadri, and M.-S. Alouini, "Front-end intelligence for large-scale application-oriented Internet-of-Things," *IEEE Access*, vol. 4, pp. 3257–3272, Jun. 2016.
[11] B. Varghese, N. Wang, S. Barbhuiya, P. Kilpatrick, and D. S. Nikolopoulos, "Challenges and opportunities in edge computing," in *Proc. IEEE Int. Conf. Smart Cloud (SmartCloud)*, Nov. 2016, pp. 20–26.
[12] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016.
[13] R. Mahmud and R. Buyya. (2016). "Fog computing: A taxonomy, survey and future directions." [Online]. Available: http://arxiv.org/abs/1611.05539
[14] S. Sarkar, S. Chatterjee, and S. Misra, "Assessment of the suitability of fog computing in the context of Internet of things," *IEEE Trans. Cloud Comput.*, to be published.
[15] S. Yi, C. Li, and Q. Li, "A survey of fog computing: Concepts, applications and issues," in *Proc. Workshop Mobile Big Data (Mobidata)*, Jun. 2015, pp. 37–42.
[16] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in *Proc. 10th Int. Conf. Wireless Algorithms, Syst., Appl. (WASA)*, Aug. 2015, pp. 685–695.
[17] I. Stojmenovic and S. Wen, "The Fog computing paradigm: Scenarios and security issues," in *Proc. Federated Conf. Comput. Sci. Inf. Syst. (FedCSIS)*, Sep. 2014, pp. 1–8.
[18] I. Stojmenovic, "Fog computing: A cloud to the ground support for smart things and machine-to-machine networks," in *Proc. Austral. Telecommun. Netw. Appl. Conf. (ATNAC)*, Nov. 2014, pp. 117–122.
[19] P. Kumar, N. Zaidi, and T. Choudhury, "Fog computing: Common security issues and proposed countermeasures," in *Proc. Int. Conf. System Modeling Adv. Res. Trends (SMART)*, Nov. 2016, pp. 311–315.
[20] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the Internet of Things: Security and privacy issues," *IEEE Internet Comput.*, vol. 21, no. 2, pp. 34–42, Mar. 2017.
[21] J. Ni, A. Zhang, X. Lin, and X. S. Shen, "Security, privacy, and fairness in fog-based vehicular crowdsensing," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 146–152, Jun. 2017.
[22] M. Xiao, J. Zhou, X. Liu, and M. Jiang, "A hybrid scheme for fine-grained search and access authorization in fog computing environment," *Sensors*, vol. 17, no. 6, pp. 1–22, Jun. 2017.
[23] M. Du, K. Wang, X. Liu, S. Guo, and Y. Zhang, "A differential privacy-based query model for sustainable fog data centers," *IEEE Trans. Sustain. Comput.*, to be published.
[24] Y. Wang, T. Uehara, and R. Sasaki, "Fog computing: Issues and challenges in security and forensics," in *Proc. IEEE 39th Annu. Comput. Softw. Appl. Conf.*, vol. 3. Jul. 2015, pp. 53–59.
[25] R. K. L. Ko *et al.*, "TrustCloud: A framework for accountability and trust in cloud computing," in *Proc. IEEE World Congr. Services*, Jul. 2011, pp. 584–588.
[26] K. M. Khan and Q. Malluhi, "Establishing trust in cloud computing," *IT Prof.*, vol. 12, no. 5, pp. 20–27, Sep. 2010.
[27] Y. W. Law, M. Palaniswami, G. Kounga, and A. Lo, "WAKE: Key management scheme for wide-area measurement systems in smart grid," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 34–41, Jan. 2013.
[28] M. A. Ferrag, L. Maglaras, and A. Ahmim, "Privacy-preserving schemes for ad hoc social networks: A survey," *IEEE Commun. Surveys Tuts.*, to be published.
[29] Y. Hong, W. M. Liu, and L. Wang, "Privacy preserving smart meter streaming against information leakage of appliance status," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 9, pp. 2227–2241, Sep. 2017.
[30] D. Koo and J. Hur, "Privacy-preserving deduplication of encrypted data with dynamic ownership management in fog computing," *Future Generat. Comput. Syst.*, to be published.
[31] S. J. Stolfo, M. B. Salem, and A. D. Keromytis, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud," in *Proc. IEEE Symp. Security Privacy Workshops (SPW)*, May 2012, pp. 125–128.
[32] M. H. Ibrahim, "Octopus: An edge-fog mutual authentication scheme," *Int. J. Netw. Security*, vol. 18, no. 6, pp. 1089–1101, Nov. 2016.
[33] N. H. Motlagh, M. Bagaa, and T. Taleb, "UAV-based IoT platform: A crowd surveillance use case," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 128–134, Feb. 2017.
[34] S. Biggs and S. Vidalis, "Cloud computing: The impact on digital forensic investigations," in *Proc. IEEE Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Nov. 2009, pp. 1–6.
[35] S. D. Wolthusen, "Overcast: Forensic discovery in cloud environments," in *Proc. IEEE 5th Int. Conf. IT Security Incident Manage. IT Forensics*, Sep. 2009, pp. 3–9.
[36] M. Peng, S. Yan, K. Zhang, and C. Wang, "Fog-computing-based radio access networks: Issues and challenges," *IEEE Netw.*, vol. 30, no. 4, pp. 46–53, Jul. 2016.
[37] M. Arrington. (Jul. 2009). *In Our Inox: Hundreds of Confidential Twitter Documents*. Accessed: Feb. 12, 2017. [Online]. Available: http://techcrunch.com/2009/07/14/in-our-inbox-hundreds-of-confidential-twitter-documents/
[38] D. Takahashi. (Mar. 2010). *French Hacker who Leaked Twitter Documents to Techcrunch is Busted*. Accessed: Feb. 20, 2017. [Online]. Available: http://venturebeat.com/2010/03/24/french-hacker-who-leaked-twitter-documents-to-techcrunch-is-busted/
[39] P. Allen. (Mar. 2010). *Obamas Twitter Password Revealed After French Hacker Arrested for Breaking into U.S. Presidents Account*. Accessed: Feb. 12, 2017. [Online]. Available: http://www.dailymail.co.uk/news/article-1260488/Barack-Obamas-Twitter-password-revealed-French-hacker-arrested.html
[40] F. Rocha and M. Correia, "Lucy in the sky without diamonds: Stealing confidential data in the cloud," in *Proc. IEEE/IFIP 41st Int. Conf. Dependable Syst. Netw. Workshops (DSN-W)*, Jun. 2011, pp. 129–134.
[41] J. Pepitone. (Jun. 2011). *Dropbox's Password Nightmare Highlights Cloud Risks*. Accessed: Feb. 12, 2017. [Online]. Available: http://money.cnn.com/2011/06/22/technology/dropbox_passwords/index.htm
[42] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, and X. Yao, "Security and privacy preservation scheme of face identification and resolution framework using Fog computing in Internet of Things," *IEEE Internet Things J.*, to be published.
[43] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for Fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, Mar. 2017.
[44] S. Basudan, X. Lin, and K. Sankaranarayanan, "A privacy-preserving vehicular crowdsensing-based road surface condition monitoring system using fog computing," *IEEE Internet Things J.*, vol. 4, no. 3, pp. 772–782, Jun. 2017.
[45] J. Liu *et al.*, "Secure intelligent traffic light control using fog computing," *Futur Gener. Comput. Syst.*, to be published.

[46] W. K. Ng, Y. Wen, and H. Zhu, "Private data deduplication protocols in Cloud storage," in *Proc. 27th Annu. ACM Symp. Appl. Comput. (SAC)*, Mar. 2012, pp. 441–446.
[47] R. Yang, Q. Xu, M. H. Au, Z. Yu, H. Wang, and L. Zhou, "Position based cryptography with location privacy: A step for fog computing," *Futur Gener. Comput. Syst.*, to be published.
[48] T. Wang *et al.*, "Trajectory privacy preservation based on a fog structure for Cloud location services," *IEEE Access*, vol. 5, pp. 7692–7701, May 2017.
[49] Y. Huo, C. Hu, X. Qi, and T. Jing, "LoDPD: A location difference-based proximity detection protocol for fog computing," *IEEE Internet Things J.*, to be published.
[50] B. Mu and S. Bakiras, "Private proximity detection for convex polygons," *Tsinghua Sci. Technol.*, vol. 21, no. 3, pp. 270–280, Jun. 2016.
[51] H. Wang, Z. Wang, and J. Domingo-Ferrer, "Anonymous and secure aggregation scheme in Fog-based public Cloud computing," *Futur Gener. Comput. Syst.*, to be published.
[52] M. Kumar, "An enhanced remote user authentication scheme with smart card," *Int. J. Netw. Security*, vol. 10, no. 3, pp. 175–184, May 2010.
[53] R. Lu, Z. Cao, Z. Chai, and X. Liang, "A simple user authentication scheme for grid computing," *Int. J. Netw. Security*, vol. 7, no. 2, pp. 202–206, 2008.
[54] L. T. Jia, "Efficient nonce-based authentication scheme for session initiation protocol," *Int. J. Netw. Security*, vol. 9, no. 1, pp. 12–16, 2009.
[55] C. C. Lee, C. H. Liu, and M. S. Hwang, "Guessing attacks on strong-password authentication protocol," *Int. J. Netw. Security*, vol. 15, no. 1, pp. 64–67, 2013.
[56] Z. M. Fadlullah, M. M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, "Toward intelligent machine-to-machine communications in smart grid," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 60–65, Apr. 2011.
[57] S. Zawoad and R. Hasan. (2013). "Cloud forensics: A meta-study of challenges, approaches, and open problems." [Online]. Available: http://arxiv.org/abs/1302.6312
[58] D. Birk and C. Wegener, "Technical issues of forensic investigations in cloud computing environments," in *Proc. 6th IEEE Int. Workshop Syst. Approaches Digit. Forensic Eng.*, May 2011, pp. 1–10.
[59] W. Delport, M. Kohn, and M. S. Olivier, "Isolating a cloud instance for a digital forensic investigation," in *Proc. Inf. Security South Africa Conf. (ISSA)*, Aug. 2012, pp. 1–7.
[60] K. Bilal, S. U. R. Malik, S. U. Khan, and A. Y. Zomaya, "Trends and challenges in cloud datacenters," *IEEE Cloud Comput.*, vol. 1, no. 1, pp. 10–20, May 2014.
[61] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities," in *Proc. 10th IEEE Int. Conf. High Perform. Comput. Commun. (HPCC)*, Sep. 2008, pp. 5–13.
[62] B. P. Rimal, E. Choi, and I. Lumb, "A taxonomy and survey of cloud computing systems," in *Proc. 5th Int. Joint Conf. INC*, Aug. 2009, pp. 44–51.
[63] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the Internet of Things: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 414–454, 1st Quart., 2014.
[64] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith, and P. Steggles, "Towards a better understanding of context and context-awareness," in *Proc. 1st Int. Symp. Handheld Ubiquitous Comput. (HUC)*, Sep. 1999, pp. 304–307.
[65] L. A. Maglaras, J. Jiang, and T. J. Cruz, "Combining ensemble methods and social network metrics for improving accuracy of OCSVM on intrusion detection in SCADA systems," *J. Inf. Security Appl.*, vol. 30, pp. 15–26, Oct. 2016.
[66] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in cloud," *Elsevier J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 42–57, Jan. 2013.
[67] J. Valenzuela, J. Wang, and N. Bissinger, "Real-time intrusion detection in power system operations," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1052–1062, Nov. 2013.
[68] S. Anwar *et al.*, "From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions," *MDPI Algorithms*, vol. 10, no. 2, pp. 1–24, Mar. 2017.
[69] T. Cruz *et al.*, "A cyber security detection framework for supervisory control and data acquisition systems," *IEEE Trans. Ind. Informat.*, vol. 12, no. 6, pp. 2236–2246, Aug. 2016.
[70] R. Marty, "Cloud application logging for forensics," in *Proc. ACM Symp. Appl. Comput. (SAC)*, Mar. 2011, pp. 178–184.

MITHUN MUKHERJEE (S'10–M'16) received the B.E. degree in electronics and communication engineering from the University Institute of Technology, Burdwan University, India, in 2007, the M.E. degree in information and communication engineering from the Indian Institute of Science and Technology, Shibpur, India, in 2009, and the Ph.D. degree in electrical engineering from IIT Patna, India, in 2015. He is currently a Specially Assigned Researcher with the Guangdong Provincial Key Laboratory of Petrochemical Equipment Fault Diagnosis, Guangdong University of Petrochemical Technology, China. His research interests include wireless sensor network, wireless communications, energy harvesting, and fog computing. He received the EAI WICON 2016 and the IEEE SigTelCom 2017 Best Paper Award. He was the Guest Editor of the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE ACCESS, the *ACM/Springer Mobile Networks & Applications*, and the *Sensors*. He has been serving as the Special Issue Editor of the *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*.

RAKESH MATAM (M'14) received the bachelor's degree in computer science from Jawaharlal Nehru Technological University at Hyderabad, Hyderabad, the master's degree from Kakatiya University Warangal, India, and the Ph.D. degree in computer science from IIT Patna in 2014. In 2014, he joined the Department of Computer Science, IIT, as an Assistant Professor. He is currently a member of the Design and Innovation Center, IIIT Guwahati, and a Principal Investigator of a funded research project sponsored by the Government of India. His research interests include wireless networks, network security, and cloud Computing. He has also served as an Organizing Committee Member in numerous international conferences.



LEI SHU (M'07–SM'15) is currently a Lincoln Professor with the University of Lincoln, U.K., and a Distinguished Professor with the Guangdong University of Petrochemical Technology. He is also the Executive Director of the Guangdong Provincial Key Laboratory of Petrochemical Equipment Fault Diagnosis, China. He has authored over 300 papers in related conferences, journals, and books in sensor networks. His main research field is wireless sensor networks. He received the Globecom 2010, ICC 2013, and the IEEE Systems Journal 2017 Best Paper Award. He has served as over 50 various co-chair for international conferences/workshops, including IWCMC, ICC, ISCC, ICNC, and Chinacom, especially the Symposium Co-Chair of IWCMC 2012 and ICC 2012, the General Co-Chair of Chinacom 2014, Qshine 2015, Collaboratecom 2017, and Mobiquitous 2018, the Steering and TPC Chair of InisCom 2015, and TPC Member of over 150 conferences, including ICDCS, DCOSS, MASS, ICC, Globecom, ICCCN, WCNC, and ISCC. He has been serving as Editor-in-Chief of the *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, and an Associate Editor of the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the *IEEE Communications Magazine*, the IEEE SYSTEMS JOURNAL, and IEEE ACCESS.

LEANDROS MAGLARAS (M'14–SM'15) received the B.Sc. degree from the Aristotle University of Thessaloniki, Greece, in 1998, and the Ph.D. degree in electrical & computer engineering from the University of Volos in 2014. He is currently a Visiting Lecturer with the School of Computer Science and Informatics, De Montfort University, U.K. He serves on the Editorial Board of several International peer-reviewed journals, such as IEEE Access, the *Wiley Journal on Security & Communication Networks*, and the *EAI Transactions on Security and Safety*. He has authored over 70 papers in scientific magazines and conferences.

MOHAMED AMINE FERRAG received the bachelor's, master's, and Ph.D. degrees from Badji Mokhtar Annaba University, Algeria, in 2008, 2010, and 2014, respectively, all in computer science. Since 2014, he has been an Assistant Professor with the Department of Computer Science, Guelma University, Algeria. Since 2010, he has also been a Researcher Member of the Networks and Systems Laboratory, Badji Mokhtar University, Annaba. He has edited the book *Security Solutions and Applied Cryptography in Smart Grid Communications* (IGI Global). His research interests include wireless network security, network coding security, and applied cryptography. He is currently serving in various editorial positions, such as Editorial Board Member of Computer Security Journals, such as the *International Journal of Information Security and Privacy* (IGI Global), the *International Journal of Internet Technology and Secured Transactions* (Inderscience Publishers), and the *EAI Endorsed Transactions on Security and Safety*. He has served as an organizing committee member (the Track Chair, the Co-Chair, the Publicity Chair, the Proceedings Editor, and the Web Chair) in numerous international conferences.

NIKUMANI CHOUDHURY (S'14) received the B.Tech degree in information technology from the Assam University, India, in 2012, and the M.Tech. degree in information technology from Gauhati University in 2014. He is currently pursuing the Ph.D. degree with IIIT Guwahati, India. He was a Project Fellow at IIT Guwahati. His research interests include low power wireless networks and Internet of Things.

VIKAS KUMAR (S'10–M'16) received the M.Tech.
degree in VLSI and CAD from Thapar University, Patiala, India, in 2008. He is currently pursuing the Ph.D. degree in electrical engineering with IIT Patna, India. He is currently a Telcom Officer with Bharat Sanchar Nigam Ltd., India. He has involved in electronic switching (EWSD, OCB, and C-DOT exchanges) and networking. His major research interests include the development of real-time communication systems, VLSI implementation for digital signal processing, and FPGA-based system design, and cloud computing.