Computers & Security 120 (2022) 102822

Contents lists available at ScienceDirect

Computers & Security

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

Insights into security and privacy towards fog computing evolution

Sabrina Sicari[a,*], Alessandra Rizzardi[a], Alberto Coen-Porisini[a]

Dipartimento di Scienze Teoriche e Applicate, Università degli Studi dell'Insubria, via O. Rossi 9, Varese 21100, Italy

ARTICLE INFO

Article history:
Received 9 June 2021
Revised 7 June 2022
Accepted 28 June 2022
Available online 30 June 2022

Keywords:
Fog computing
Internet of things
Security
Privacy
Cloud computing
Fog networking

ABSTRACT

The incremental diffusion of the Internet of Things (IoT) technologies and applications represents the outcome of a world ever more connected by means of heterogeneous and mobile devices. IoT scenarios imply the presence of multiple data producers (e.g., sensors, actuators, RFID, NFC) and consumers (e.g., end-user devices, such as smartphones, tablets, and PCs). A variety of standards and protocols must cooperate to efficiently gather, process, and share the information. The fog computing paradigm, due to its distributed nature, represents a viable solution to cope with interoperability, scalability, security, and privacy issues, which naturally emerge, since it operates as an intermediate layer between data consumers/producers and traditional cloud systems. This paper analyzes the evolution in the modeling of new methodologies, related to fog computing and IoT, showing how moving security and privacy tasks toward the edge of the network provide both advantages and new challenges to be faced in this research field. The proposed discussion provides an overview of requirements for the realization of secure and privacy-aware IoT-based fog computing infrastructures.

1. Introduction

Fog computing, which is also known as *fog networking* or *fogging*, mainly consists of a decentralized networking and computing infrastructure, where data, processing tasks, storage and applications are distributed in an efficient manner between the data sources and the cloud. It is promoted by the OpenFog Consortium (0000) (now merged into the *Industrial Internet Consortium*), which encourages many initiatives all over the world about the diffusion of fog computing design solutions. The notion of fog computing essentially moves most of the cloud computing tasks and the cloud services towards the edge of the network, bringing the advantages and potentialities of the cloud closer to where data are effectively acquired, elaborated, and shared (Mouradian et al., 2017). In a few words, certain application processes and services are managed at the edge of the network by one or more smart devices (or smart gateways or routers), but others are still managed by the cloud (i.e., the most costly). More in detail, the following tasks are mainly performed by the "fog" layer of the network: (i) the provision of processing and memory resources to edge devices; (ii) the pre-processing of the collected data; (iii) the transmission of aggregated results to the cloud. Whereas the cloud has the responsibility to supervise the managed systems and make reports and further investigations on the aggregated results received by the smart devices (Dillon et al., 2010).

Hence, the main goal of fogging is to improve efficiency and reduce the amount of data transmitted to the cloud for processing, analysis, and storage. Other advantages are related to the security and privacy of the data (Martin et al., 2017). In fact, the cloud often represents a single point of failure, and users and interested parties who/which want to use the data stored and processed there should consider the cloud platform itself trusty (Abbadi and Martin, 2011); while, with the adoption of a fog layer, a new security level could be added. For example, the decentralization, brought by the fog layer, would allow the diffusion of new design methodologies, which should enable and encourage the control of the data by the owners themselves; so they should be equipped with the necessary means for establishing, in an autonomous or semi-autonomous way, how to share their information. In such a scenario, the main issues are related to the following topics: authentication of users and devices, access control on network resources, data integrity and confidentiality, key management, trust, attacks' detection, anonymity, and privacy (Sicari et al., 2015).

Moreover, as both enterprises and private citizens are increasingly adopting Internet of Things (IoT) solutions, it becomes clear that current cloud computing systems will not be able to handle a whole load of data by themselves, thus fog computing comes, again, into play. Note that the utilization of technologies and protocols related to the IoT paradigm is now continuously spreading in many application contexts, from the smart home to the smart

[*] Corresponding authors.
E-mail addresses: sabrina.sicari@uninsubria.it (S. Sicari), alessandra.rizzardi@uninsubria.it (A. Rizzardi), alberto.coenporisini@uninsubria.it (A. Coen-Porisini).

https://doi.org/10.1016/j.cose.2022.102822
0167-4048/© 2022 Elsevier Ltd. All rights reserved.

city, to the e-health, the smart traffic management, the smart agriculture, military fields, and so on (Miorandi et al., 2012). Some scenarios are already targeted by fog networking, such as smart grids, smart buildings and cities, vehicle networks, and building blocks, such as software-defined networks (SDN) and network function virtualization (NFV) (Mouradian et al., 2017). In the IoT vision, everyday objects are equipped with sensing and actuation capabilities, in order to get connected to a globally networked infrastructure, supporting the provisioning of innovative and customized services to individuals and businesses. Such objects are named *smart things* and are able to interact among themselves and with the surrounding environment, to fulfill a common goal, depending on the specific application domain. The resulting system may include an extremely large number of heterogeneous devices (e.g., wireless sensor networks, actuators, RFID, NFC, etc.), raising integration and scalability challenges to be addressed, due to the coexistence of different standards and protocols. Moreover, security and privacy requirements involve such a huge amount of scattered IoT devices, which, from the one side, must be protected against violation attempts (e.g., data leakage, data confidentiality and integrity violation, identity theft); while, on the other side, the presence of malicious objects in the IoT network must be prevented and counteracted (Butun et al., 2019). Note that the real business value enabled by the IoT technologies is derived not totally from the data, but also from the added mechanisms, which facilitate real-time actions, efficiency, reliability, and utilization, closer to the user-side (Lee and Lee, 2021).

From the just presented analysis, naturally emerges the need for modeling a proper network infrastructure, able to manage the huge amount of information gathered and transmitted by the *smart things*, in a very dynamic environment. The spreading of IoT architectures and applications is also encouraged by the benefits brought by 4G technologies, and also by the advent of 5G (Li et al., 2018b), which is about to be installed in many cities (Kitanov et al., 2016). As a consequence, fog computing can potentially act a fundamental role in solving the main issues to concur to the design and development of an efficient and security-aware IoT infrastructure (Román-Castro et al., 2018). Current IoT security solutions at the edge layer could inspire more edge-based IoT security designs, as discussed in Sha et al. (2020).

Summarizing, the advent of fog computing should provide new functionalities and ways of managing the data, in order to address the following fundamental requirements: efficiency of data retrieval, scalability, interoperability, security, and privacy. In this paper, we investigate, analyze, and discuss the importance and the evolution of fog computing design solutions in the IoT, from a security and privacy perspective. With respect to existing surveys, the focus of this work is on the fog computing IoT-based network infrastructure, which adds a further layer to the cloud and/or edge computing-based architectures Khan et al. (2017) Roman et al. (2018). Moreover, all the aspects related to security are examined: not all of them have been deepened enough in the literature within fog computing-based scenarios Mukherjee et al. (2017) Ni et al. (2017). Such considerations are detailed in Section 2, which presents the existing surveys, studies, and tutorials on security and privacy in fog computing, pointing out the current state of the art in this field. As hereby demonstrated, in the literature a comprehensive study that directly focuses on the design and development of security and privacy solutions for fog computing in the IoT still lacks. From such a conclusion, it derives the main contribution of our paper. Section 3 proposes a comparison between cloud and fog computing paradigms, mainly from a security and privacy perspective. Section 4 points out the relation between fog computing and the IoT, distinguishing among solutions and ongoing projects, which take into account security and privacy requirements or not. Section 5 analyzes and discusses the security and privacy issues that emerged in the design of fog computing solutions in IoT scenarios. The emerged considerations outline advantages and challenges and represent future research directions, which should be of interest to various audiences, including most notably Ph.D. candidates, research consortia, and the IT industry. Finally, Section 6 summarizes the outcomes of the conducted research.

2. Motivation, emerging issues and related work

Note that several surveys, studies, and tutorials have been already proposed in literature about fog computing. Many of them do not cover security and privacy aspects, since they focus on the other main topics, such as: (i) fog architectures and platforms (Alli and Alam, 2020; Fahmideh and Zowghi, 2020); (ii) fog use cases (Avasalcai et al., 2020); (iii) evaluation criteria for the fog systems (Hu et al., 2017a; Martinez et al., 2020; Mouradian et al., 2017); (iv) mobility (Luan et al., 2015; Puliafito et al., 2017; Rejiba et al., 2019); (v) orchestration (Costa et al., 2022; Mahmud et al., 2018; Wen et al., 2017).

Otherwise, hereby a review on prior works is provided, in order to make a comparison with the proposed research analysis, revealing covered aspects and shortcomings. Moreover, the following discussion puts in light the security and privacy issues and requirements in fog computing environments.

The study in Yi et al. (2015a) describes some specific application scenarios related to fogging, such as augmented reality and real-time video analytics, web content delivery and caching, and mobile big data analytics. It also identifies the main Quality of Service (QoS) metrics for fog services, which are: connectivity, reliability, capacity, and delay. With regards to security and privacy, the following issues are pointed out: authentication, access control, and intrusion detection. More in detail, biometric-based authentication, such as fingerprint authentication, face authentication, touch-based or keystroke-based authentication, could be adopted to realize a trusted execution environment (TEE), so that executed tasks and data inside a fog computing system (or a part of it) could be considered protected; however, no clear motivations of performance evaluation are provided to support such a thesis. Similarly, access control is treated superficially. In general, effective solutions should aim to guarantee access control among client devices, fog devices, and the cloud, reducing as much as possible computation costs and delays, thus meeting the resource constraints of the involved devices. Concerning intrusion detection, it is distinguished in two parts: (i) intrusion detection on the device/system side; (ii) intrusion detection on the network side. The former can include insider attacks, such as flooding attacks, port scanning, attacks on VM or hypervisor; the latter usually aims to detect activities such as denial-of-service (DoS). In fog computing, new challenges to face intrusion detection are related to the high mobility of end-devices, the large-scale environment, and geo-distribution information. Such issues are not still addressed, due to the complexity of the management of devices' authorization and the trustworthiness of the IoT underlying platform.

To partially cope with such an emerged issue, the work in Mahmud et al. (2018) presents a taxonomy of the following aspects related to fog computing: fog nodes' configuration, nodal collaboration (i.e., cluster, peer-to-peer, master-slave), resource/service provision's metrics (e.g., delays, costs, energy consumption), the intermediary role of Service Level Objectives (SLOs), applicable network systems (e.g., IoT, mobile networks, radio access networks, content distribution networks), security concerns. With regards to security, the following topics are mentioned: authentication, encryption, privacy, and DoS attacks. Even if, such aspects of security are not deeply discussed, and the conclusions are superficial, the authors state that authentication should not be limited to users, but should be extended to devices, data migration, and instances.

To continue with security-related issues, in Alrawais et al. (2017a), the following features are pointed out and discussed as open challenges in the design of fog computing/IoT solutions:

- *Authentication.* The authors point out that traditional public-key infrastructures (PKI) do not scale in IoT systems.
- *Trust.* The authors envision the building of a trust model based on reputation.
- *Rogue Node Detection.* The authors claim that a trust measurement-based model could be applied to detect rogue nodes in IoT environments.
- *Privacy.* The resource-constrained IoT devices limit the techniques that can be adopted to guarantee efficient and effective privacy-preserving schemes. The main issue related to the users' privacy in the IoT is related to location, since many IoT applications are location-based services, especially if they are accessed by means of mobile devices.
- *Access control.* The main challenge is managing access to resources in presence of highly distributed data.
- *Intrusion detection.* The key challenge for intrusion detection is how to design a detection system able to run in large-scale, widely geo-distributed, and highly mobile environments.
- *Data Protection.* The authors claim that data must be preserved not only at the communication level (i.e., during network transmissions), but also at the processing level, when information is physically stored on a device or in the cloud.

It is worth remarking that the authors of Alrawais et al. (2017a) point out the importance of location-awareness both for guaranteeing privacy, since IoT data are usually based on data acquired in certain network's places, and for detecting attacks and malicious devices. The situation is further complicated in presence of mobility for the involved end-devices, because the network's configuration evolves during the time, making it difficult to recognize misbehaviors at a certain node or ensuring the synchronization of privacy-preserving schemes.

The paper proposed in Khalid et al. (2021) reviews the existing privacy and access control schemes in fog computing, while the one presented in Lee et al. (2015) explains how the adoption of fog computing into IoT environments introduces several unique security threats. The following outcomes emerge:

- Proper security countermeasures must be put in action to protect the IoT network communications, which take place among IoT devices, fog nodes, and the cloud. In the authors' opinion, traditional authentication and secure information flows' systems do not suit the new needs of fog architecture.
- Fog nodes must support different standards and protocols to communicate with IoT devices; hence, multi-OS environments become essential, as well as the adoption of virtualization technologies to allow cooperation and integration. In such a context, the spreading of wrong data may not be controlled; hence, real-time monitoring of fog nodes should be put in the act. However, the performance overhead of such a dynamic analysis is high. Also high is the put in action of intrusion detection systems, which could help in recognizing possible attackers. A typical attack consists in exporting or altering important information with the acquisition of higher privileges, obtained by exploiting some vulnerabilities of the virtualization technology.
- IoT devices are the most vulnerable to security threats since information leakage can improperly access users' sensitive information, such as habits or preferences. In this way, users' behavior could be predicted, compromising the privacy.
- Fog nodes should trust the cloud system, since the cloud handles fog nodes' authentication and manage their participation in the fog environment.

Note that the authors of Khalid et al. (2021) put in light another interesting point, especially for scenarios that require strict constraints in terms of response time: the efficiency in real-time data retrieval. This aspect is not only fundamental for information dissemination, but also for detecting attacks. For such a reason, monitoring and logging activities are crucial for guaranteeing robustness and reliability in a fog computing-based infrastructure, as detailed in Section 5.

Such studies clarify the main challenges related to security in privacy in fog computing, ranging from authentication, to access control, data protection, trust towards the network architecture, attacks, and intrusion detections. Instead, other papers put security in relation to the peculiarities of the network infrastructure, as follows.

For example, a survey on fog computing within SDN is presented in Salman et al. (2018). Concerning security, the authors consider five main aspects: identity management, authentication, access control, trustworthiness, and privacy. In particular, they show how SDN/NFV can be employed to overcome the security challenges in the IoT and how it serves in the development of security-embedded architectural solutions. However, at the same time, the authors point out that the introduction of SDN brings new security challenges to be faced, such as: (i) the presence of a single point of failure, due to the centralization of the intelligence at the controller level; (ii) the exposure of the controller to DDoS attacks; (iii) switches can be hijacked, thus inconsistent rules can be added compromising the network availability; (iv) the interaction with third-party unauthenticated applications.

The manuscript presented in Laroui et al. (2021) analyzes recent research activities like task scheduling, SDN/NFV, security and privacy and the blockchain in edge and fog computing for IoT. Concerning security, the authors consider authentication, data protection, and preventing cache attacks as pillars for guaranteeing an adequate level of reliability to managed information. Moreover, some solutions adopting blockchain in edge computing systems are described: here the main issue is how to deal with the resources (i.e., computing effort, storage, energy consumption) required by the blockchain concerning the constrained IoT devices.

The overview presented in Vaquero and Rodero-Merino (2014) mainly focuses on the involved technologies and connectivity in fog architectures. In particular, the efforts to be done for allowing efficient data exchanges are put in relation with the available wireless access technologies in WAN, MAN, and LAN. LTE and 4G expand the available bandwidth at the edge networks, thus facilitating devices connectivity; while short-range technologies, requiring devices to organize themselves, are ever increasingly spreading, such as Bluetooth, low energy, ANT+, ZigBee and RF4CE. Security is superficially treated from a privacy viewpoint, underlying that a solution is to store encrypted sensitive data in traditional clouds. However, such a method makes it hard to perform any processing over such data. Such an aspect will be discussed in detail in Section 3.

The study in Roman et al. (2018) first provides an overview of the different network approaches, which leverage the principles of the edge computing paradigm, such as Mobile Edge Computing (MEC), Mobile Cloud Computing (MCC), and fog computing; then, the paper points out the security threats, distinguishing them on the basis of the target of the attack, as follows:

- Network infrastructure, which implies the DoS, the man-in-the-middle attack, the rogue gateway;

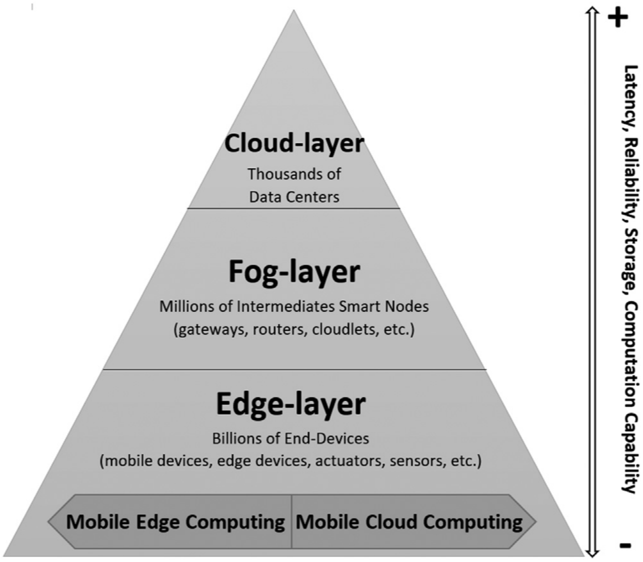
Cloud-layer
Thousands of Data Centers
Fog-layer
Millions of Intermediates Smart Nodes (gateways, routers, cloudlets, etc.)
Edge-layer
Billions of End-Devices (mobile devices, edge devices, actuators, sensors, etc.)
Mobile Edge Computing
Mobile Cloud Computing
+
Latency, Reliability, Storage, Computation Capability
-

Fig. 1. Relation among fog computing, MEC and MCC.

- Edge data center, which implies the physical damage, the privacy leakage, the privilege escalation, the service manipulation, the rogue data center;
- Core infrastructures, which imply the privacy leakage, the service manipulation, the rogue infrastructure;
- Virtualization infrastructure, which implies the DoS, the misuse of resources, the privacy leakage, the privilege escalation, the virtual resources' manipulation;
- User devices, which imply the malicious data injection, the service manipulation.

Note that such work does not refer to the IoT. Such an aspect is the main difference between Roman et al. (2018) and our proposed work; moreover, the focus of our paper is on fog computing, not on other edge computing-based paradigms (e.g., MEC and MCC). It is worth remarking that edge computing is essentially adopted when data computation is performed at the networks edge, in close proximity to the physical location acquiring the data, while fog computing acts as a mediator between the edge and the cloud for various purposes, such as data filtering. Hence, fog computing cannot replace edge computing, while edge computing can live without fog computing in many applications. Moreover, fog computing adds a further layer to the network architecture, so it is a more complex system that needs to be integrated with current infrastructures, even if it requires investment for IT companies. The same considerations can be pursued for the survey detailed in Khan et al. (2017). Fig. 1 sketches the relation among fog computing, MEC, and MCC. Also, the work in Mukherjee et al. (2017) is not tailored to the IoT, but to security and privacy issues in fog computing in general. The following security-related requirements are considered: trust, authentication, secure communications, end-user privacy, and malicious attacks. No in-depth discussion is provided about how to solve the emerged challenges, and future research directions are not outlined, as we do in our work. The same is for the work proposed in Yi et al. (2015b), which treats the same topics of Mukherjee et al. (2017), but, in addition, it discusses verifiable computing and data search, as techniques for guaranteeing secure and private data processing on encrypted information. Such a paper also distinguishes between data privacy, user privacy, and location privacy. The first is strictly related to the disclosure of sensitive information by the fog devices; the second is related to the monitoring of users' habits in interacting with the fog devices; while the third is related to the detection of information related to the users' movements, or to the fog devices' relationships into the network.

A comprehensive architectural survey is provided in Habibi et al. (2020), where current reference architectures and major application-specific architectures describing their salient features and distinctions in the context of fog computing are explored. More in detail, base architectures for application, software, computing resource management and networking are presented. Also, security is marginally discussed from an architectural viewpoint; in fact, the authors distinguish in access layer security, fog layer security, and fog-cloud interconnection security, only pointing out the major attacks on a fog computing ecosystem based on the standard ISO 27001. Similarly, the work in Mostafavi and Shafik (2019) focuses on privacy breaches in fog architectures.

Concerning the possible attacks, the study in Stojmenovic and Wen (2014) surveys a typical attack that can occur in fog computing: the man-in-the-middle. More in detail, the stealthy features of such an attack are investigated by examining its CPU and memory consumption on a fog device. The paper also describes the advantages of fog computing in satisfying the requirements of applications, such as smart grids, smart traffic lights and connected vehicles, wireless sensor and actuator networks, decentralized smart building control, IoT and Cyber-physical systems (CPSs). Such requirements consist in scalability, interoperability and reliability.

Finally, the survey, presented in Ni et al. (2017), represents a very complete and extended analysis of the role of fog computing in various IoT applications; moreover, the authors propose a wide discussion about fog features, and comparison between fog and cloud computing from many viewpoints. Concerning security and privacy, different requirements are analyzed and put in relation to existing approaches; however, such approaches are not always specifically targeted to fog computing, but to IoT or traditional networks, in general. In this sense, our work aims to be more focused on strict security and privacy features of fog computing in the IoT than the work in Ni et al. (2017).

Summarizing, investigated works cover the main topics shown in Table 1.

Instead, Table 2 provides a more detailed comparison between the proposed research and the discussed existing studies and survey papers. In this way, the motivations supporting the study conducted in this paper emerge along with the above discussion about available surveys and tutorials. It is worth remarking that studies in Table 2 are arranged in reverse chronological order. More recent works mainly focus on architectural aspects and application scenarios of fog computing, instead of focusing on security (e.g., Habibi et al. (2020), Mostafavi and Shafik (2019), Roman et al. (2018)); while older papers that focused on security issues in fog computing do not discuss more innovative solutions and only partially deal with all the security and privacy requirements (e.g., Lee et al. (2015), Stojmenovic and Wen (2014), Vaquero and Rodero-Merino (2014)). Many issues related to the modeling of secure and privacy-aware solutions for the fog computing adoption in IoT network architectures emerged from literature (e.g., Alrawais et al. (2017a), Mukherjee et al. (2017)); in this paper, we want to blend them, in order to reveal the pressing needs and to pave the way to a wide diffusion of fog-based applications, both targeting academic types of research and industry. In the authors' opinion, such topics have a fundamental importance in the IoT era, where more and more devices are connected every time to the network and, in particular, to the Internet. In order to enable the diffusion of innovative and efficient applications, it is also important to design reliable solutions, able to protect the users' information, as well as the disclosure of the data (maybe sensitive), which are managed by the IoT infrastructure. From the analysis hereby conducted, we derive the following security requirements, which will be detailed in Section 5: (i) the importance

Table 1
Aspects treated by surveys and tutorials about fog computing.

Main topic	Works
IoT	Alrawais et al. (2017a) Lee et al. (2015) Mahmud et al. (2018) Ni et al. (2017) Puliafito et al. (2017) Salman et al. (2018) Stojmenovic and Wen (2014) Wen et al. (2017)
architectural aspects	Hu et al. (2017a) Mahmud et al. (2018) Mouradian et al. (2017) Wen et al. (2017) Mostafavi and Shafik (2019) Habibi et al. (2020)
technologies and connectivity	Vaquero and Rodero-Merino (2014)
mobility	Luan et al. (2015) Puliafito et al. (2017)
use cases	Hu et al. (2017a) Laroui et al. (2021) Mouradian et al. (2017) Stojmenovic and Wen (2014) Yi et al. (2015a)
security and privacy	Alrawais et al. (2017a) Khalid et al. (2021) Khan et al. (2017) Lee et al. (2015) Mahmud et al. (2018) Mostafavi and Shafik (2019) Mukherjee et al. (2017) Ni et al. (2017) Roman et al. (2018) Salman et al. (2018) Stojmenovic and Wen (2014) Yi et al. (2015a) Yi et al. (2015b)

Table 2
State of the art analysis in reverse chronological order.

Work / Year	Main content/scope	Security requirements discussed
This work	evolution of security and privacy methodologies for fog computing in the IoT	encryption, key management, access control, anonymity, privacy, trust, rogue node detection, attack detection
Khalid et al. (2021)	privacy and access control schemes in fog computing	privacy, access control, trust
Laroui et al. (2021)	edge and fog computing for IoT applications	authentication, privacy, blockchain
Habibi et al. (2020)	fog computing architectural aspects	distinction in access layer, fog layer, and fog-cloud interconnection security
Mostafavi and Shafik (2019)	identification of privacy breaches in fog computing architectures	privacy, trust
Roman et al. (2018)	network approaches in edge computing	privacy, rogue node detection
Mahmud et al. (2018)	fog computing taxonomy	authentication, encryption, privacy, DoS attack
Salman et al. (2018)	fog computing in SDN	identity management, authentication, access control, trustworthiness and privacy
Ni et al. (2017)	role of fog computing in IoT applications	identity management, authentication, access control, intrusion detection, trust
Alrawais et al. (2017a)	security&privacy issues in fog computing for the IoT	authentication, trust, rogue node detection, privacy, access control, intrusion detection, data protection
Khan et al. (2017)	current applications and security solutions in edge computing	privacy, authentication, encryption, data theft
Mukherjee et al. (2017)	challenges concerning security and privacy in fog computing	trust, authentication, secure communications, end-users' privacy, malicious attacks
Yi et al. (2015a)	QoS metrics for fog services, specific application scenarios (e.g., big data, augmented reality)	authentication, access control, and intrusion detection
Lee et al. (2015)	issues in adopting fog computing into the IoT	authentication, intrusion detection, information leakage, trust
Stojmenovic and Wen (2014)	fog computing advantages in different scenarios	man-in-the-middle attack
Vaquero and Rodero-Merino (2014)	technologies and connectivity in fog architectures	encryption, privacy

of encryption mechanisms for preserving data confidentiality and integrity; (ii) encryption must be supported by clever key management techniques to guarantee the robustness against possible threats; (iii) access control, which is mainly based on authentication and authorization mechanisms; (iv) sensitive data and identity protection, which can be pursued by means of anonymity and privacy-aware schemes; (v) trust among the systems' components is very difficult to establish, mainly in presence of rogue nodes, which can hinder the reliability of information; (vi) the definition of intrusion and attack detection methods is fundamental to prevent misbehavior within the network. Such aspects must be taken into account, and the research is not mature enough to guarantee robust approaches, thus various open challenges will be pointed out in Section 5, along with hints for possible solutions.

3. Fog and cloud computing

In this section, the features of fog and cloud computing paradigms are presented, along with considerations about the application scenarios. Such a discussion is crucial for assessing new design choices and methodologies in the investigated field.

3.1. Main requirements

In order to clearly understand the real advantages and main issues related to the adoption of the fog computing paradigm, it is important to point out that fogging, in some ways, derives from cloud computing principles. In particular, fog computing aims to represent a sort of distributed cloud. Both of them have the same main goal: providing distributed storage, applications, and data to end-users.

Cloud computing has been conceived as a way of sharing resources, services and data among the interested devices or users on demand by means of any kind of device (e.g., computers, tablets, smartphones) over the Internet. Instead, fog computing mainly exploits the local computing resources of smart devices (e.g., sensors, actuators, mobile devices) rather than accessing remote servers' resources, thus reducing latency and increasing performance efficiency. While edge devices are located where data are really generated and collected, they do not have the computing and storage resources to perform advanced analysis and machine-learning tasks. Though cloud servers have the power to do such tasks, they are often too far away to process the data and respond promptly. In a fog environment, the processing task takes place on smart devices, or in smart routers or gateways, thus reducing the amount of data sent to the cloud and, as a consequence, the response times. It is important to note that fog networking is complimentary, but not replaces, cloud computing; in fact, fogging handles short-term analysis at the edge of the network; while the cloud performs resource-intensive, longer-term analysis on dedicated and powerful servers. As emerged in Section 2, two key requirements behind the need for fog computing-based applications are location-awareness and real-time data retrieval. In this sense, clouds totally lack location-awareness (being a centralized entity), and latencies naturally emerge due to the huge amount of data, processing tasks, and "distance" of connectivity of cloud from end-users.

In addition, the fact that all endpoints, connecting to and sending "raw" data to the cloud, over the Internet, can have security and privacy implications, especially when dealing with sensitive information. Note that cloud computing and storage solutions are third-party data centers, which are, as just said, usually located far from the users' action range. As a consequence, the users have to accept the treatment conditions when they use cloud services/applications or provide personal data. Naturally, cloud-based systems offer proper levels of security and privacy (Singh et al., 2016), as well as policies, that regulate the disclosure of the managed information. However, users have to trust the service providers (Abbadi and Martin, 2011), which, in turn, can access the data that is in the cloud at any time, delete or modify them (also accidentally), and share information with third parties, even without the agreement of the users. To cope with such issues and prevent unauthorized access, users can encrypt the data before providing them to the cloud system, but often it is not possible or sufficient. Such a situation is due to the fact that the adopted encryption schema (also those based on homomorphic encryption (Atayero and Feyisetan, 2011)) or the chosen encryption keys may be weak and, thus, they may be easily compromised by external malicious entities. Moreover, keys have to be kept on a separate storage block concerning the encrypted data, as well as, a system for the backup of the keys is needed, in case such a storage block is attacked. Also, the keys should automatically expire after a period of time and a refresh schedule should be handled. Obviously, such aspects require, from the cloud management perspective, a further effort (Fernandes et al., 2014).

Last but not least, information taken from a cloud can be also sent to users' mobile devices, which, in turn, must own the decryption keys, if the data are encrypted, in order to access them. Such a feature may be not desirable since mobile devices are overly vulnerable in terms of security, because mobile devices can be easily tampered. Moreover, due to resource constraints of mobile devices (e.g., computation capacity, battery lifetime, and storage capacity), mobile users are not able to attain ad adequate quality of experience. To cope with such an issue, MCC has been introduced: mobile cloud applications move the computing power and data storage away from mobile devices into the cloud. Then, mobile devices communicate with the cloud with the help of base stations, access points, or satellites. Unfortunately, MCC suffers from long latencies, particularly due to the dramatic increase in todays traffic loads. To overcome such a limitation, researchers and network engineers have developed innovative solutions tailored to offload parts of the computation from the cloud to a surrogate device in the vicinity of the end-user. Such solutions are generally referred to as *edge computing*, take advantage of location-awareness, and can provide a far more timely response. In this field, MEC is a particular form of edge computing where a cloud server is running at the edge of the cellular networks and its role is performing tasks, such as augmentation of application performance and reduction of network congestion. A MEC platform allows computation and services to be hosted at the network edge, which reduces the total latency and bandwidth consumption (Habibi et al., 2020). The fog computing paradigm leverages a different network architecture that uses near-end user edge devices to carry out the processing, control, configuration, measurement, and management tasks. It is based on a scenario where a huge number of heterogeneous ubiquitous and decentralized devices collaboratively perform network functions or applications. In this scenario, fog nodes form the physical infrastructure that provides resources for services at the edge and in the network. Hence, the idea in edge computing is to push data processing to the data source as much as possible, while fog computing provides a more general framework where a multitude of edge devices collaboratively provide the necessary computing platform. The advantages of fog computing include: (i) bandwidth savings, since data can be processed locally instead of sending them to the cloud; this will be especially beneficial when increasing the number of IoT devices; (ii) latency savings, because data can be processed at the nearest data source geographically closer to the user; this can produce instant responses especially for the time-sensitive services; (iii) better privacy, because users data are analyzed locally instead of sending them to the cloud. Hence, fog computing brings the opportunity to efficiently operate over large geography more securely, thanks to the pervasive distribution of fog nodes. Organizations and ongoing projects could surely improve their decision-making process, speed up the deliverance of data, and maintain consistency in relayed data.

The focus of this paper is on fog computing infrastructure. Due to its complexity, proper solutions must be defined, in order to cope with some critical aspects: tasks' scheduling, interoperability and scalability in presence of multiple and heterogeneous data producers and consumers, authentication, trust and encryption. Fog computing principles already address the data retrieval efficiency issue and try to cope with the other challenges, coupling to the emerging IoT contexts (Bonomi et al., 2012), as explained in Section 4. In fact, the IoT principles resemble the need for ubiquitous connectivity, mobility, heterogeneity, and dynamism of the actual network's contexts. In the next section, we deepen some relevant application scenarios in the IoT/fog computing field.

3.2. Application scenarios

Taking into account the requirements and issues that emerged from the state of the art, the application scenarios presented hereby point out traversal requirements that must be taken into account when designing an IoT/fog computing system. Relevant issues to be solved include: reducing the communication delays, enabling the interplay among the heterogeneous kinds of devices involved in the network, distributing the processing load and storage. We intend to provide, in this way, a wider view of the possibilities and the challenges concerning the adoption of the fog computing paradigm to the interested audience.

Note that many IoT context are influenced by fog computing, such as: healthcare (Stantchev et al., 2015) and telemedicine (Dubey et al., 2015) systems; smart cities (Naranjo et al., 2018; Tang et al., 2015); smart grids (Okay and Ozdemir, 2016); smart urban surveillance (Chen et al., 2016); vehicular computing (Sookhak et al., 2017; Truong et al., 2015). A platform for smart living, including smart energy, smart office, smart healthcare, smart protection, smart entertainment, and smart surroundings is envisioned in Li et al. (2015). It consists of: (i) fog nodes, represented by IoT devices; (ii) fog edge nodes (e.g., smartphones, access points, routers, switches), aiming to provide to the smart IoT objects processing, storage and communication capabilities; in fact, they should provide a variety of wired and wireless access methods to empower immediate communication with IoT devices; they also perform decision-making and action-taking to allow real-time interactions; (iii) fog servers, which focus on the interplay among fog edge nodes and the cloud. Another integrated solution, based on fog computing, cloud, and the IoT architectural paradigm which is claimed to have potential application in smart cities, intelligent transportation systems, localized weather maps and environmental monitoring, and real-time agricultural data analytics and control, is proposed in Munir et al. (2017).

Further solutions cope with other specific scenarios, such as: in the industrial IoT, a service popularity-based smart resources partitioning scheme is proposed Li et al. (2018a); Constant et al. (2017) proposes, develops and validates a smart fog gateway to perform an end-to-end analysis on the data obtained by internet-connected wearable devices; Zao et al. (2014) focuses on augmented brain-computer interactions, based on fog computing.

The study in Bonomi et al. (2012) demonstrates the role of fogging in three typical IoT scenarios: connected vehicles, smart grids, and wireless sensor and actuator networks (WSAN). The connected vehicles' context includes vehicle-to-vehicle communications, vehicle-to-access point interactions, or access point-to-access point connectivity, which usually implies Wi-Fi, 3G, LTE, roadside units protocols. Relevant application examples are those of smart lights, traffic support, info-entertainment services, safety, analysis of geo-distribution of vehicles and people, mobility and location awareness. The following requirements are fundamental: low latency, heterogeneity of devices/ information gathered, and support for real-time interactions. The same considerations can be done for smart grids and WSAN. Likewise, the work proposed in Lee et al. (2016) is targeted to WSAN, and presents a gateway-based fog computing architecture by means of a conceptual model.

A fog computing-based framework for data-driven machine health and process monitoring in cyber-manufacturing is introduced in Wu et al. (2017). The solution consists of four elements: a workflow, a certain number of wireless sensor networks, some communication protocols, and some predictive analytic methods. An online process monitoring system, which is in charge of collecting real-time machine condition data and monitoring the vibrations and energy consumption of pumps, is described through a case study. Also, a machine learning algorithm is integrated, in order to create predictive models on scalable high-performance computing resources. In line with the previous approach, also Gia et al. (2015) is focused on electrocardiogram (ECG) feature extraction as a case study. A test-bed has been deployed, to calculate parameters, such as latency, data-rate, data size, and link quality.

What emerges from such an analysis is that fog computing can be adopted in many different applications domains, with similar requirements in terms of networks' performance. Such works point out useful aspects to be taken into account in the realization of security and privacy-aware approaches, such as architectural aspects, connectivity, resources' management and identification, data processing, algorithms for data analysis, scalability, location-awareness, interoperability and efficiency (e.g., in terms of latencies, costs, and so on), which must be considered also when security and privacy mechanisms are integrated into the network infrastructure, mainly in presence of constrained IoT devices (e.g., sensors, actuators).

4. Fog computing and Internet of Things

Today, as many enterprises and large companies and organizations, as well as private citizens, are beginning to adopt IoT technologies for their usual activities, the need for large amounts of data to be accessed more quickly, locally, and in a security-aware manner, is ever-growing. Another critical issue is related to the power and resources' constraints of IoT devices, which prevent them from performing heavy processing tasks, both related to data elaboration and security operations. Fog computing, in presence of a multitude of interconnected IoT-enabled devices, can help in reducing energy consumption on such devices and network latency, by minimizing the time required for data processing (thus improving data retrieval efficiency) and for producing quick responses to the requester (Puliafito et al., 2019). In this section, we put in light if and how the available design approaches deal with security and privacy requirements.

4.1. Research methodology

Hereby we consider the security and privacy features, which emerged from the state of the art in Section 2, grouped as follows: (i) data integrity and confidentiality, guaranteed by means of cryptographic primitives and aimed at data protection; (ii) key management techniques, if available; (iii) authentication and authorization mechanisms, which should provide robust management of the access to the IoT resources; (iv) privacy of data contents and users by design, putting in act proper policies; (v) mechanisms to determine the level of trust among the entities participating to the network's activity; (vi) intrusion detection, realized by actuating proper attacks' recognition measures. Such groups have been used to outline the research throughout the literature. In particular, we analyzed the papers belonging to the last 10 years (i.e., from 2012 to 2021) from *Google Scholar, ScienceDirect* and *Scopus* by searching the following keywords: *"fog computing" && "internet of things" && ("security" || "authentication" || "authorization" || "access control" || "integrity" || "confidentiality" || "encryption" || "key management" || "privacy" || "security policies" || "intrusion detection" || "intrusion trust")* Results included both research papers and review articles (e.g., surveys). Hence, we distinguished them on the basis of the type of research: research papers would have been candidates to be included in Section 4.2, whereas review articles would have fitted into Section 2. Some papers selected for the discussion in Section 4.2 have been derived from the found review articles.

We noticed that solutions concerning authentication also included authorization and/or access control and vice versa, due to the fact that access control policies are reflected in the authentication of users to resources and authorization on the execution of tasks over them; moreover, when confidentiality was discussed, also integrity was seamlessly considered and both of them involve encryption techniques; privacy is usually a stand-alone topic, while intrusion detection is always coupled with possible threats. After a preliminary analysis of the results, we decide to include in our discussion the papers (published in journals or conference proceedings) focused on the aforementioned security requirements in IoT/fog computing environments/architectures. In particular, we examined more than 100 papers published in international scientific journals and more than 60 papers belonging to conference proceedings. Then, we excluded about 30 journal papers and 30 conference papers on the basis of the following criteria: (i) quality of the research in terms of publication type (i.e., the international importance of the journal or the conference, authors' curriculum); (ii) relevance and appropriateness with the context of interest (i.e., papers mainly focused on edge or cloud computing without significant contribution in terms of security have been discarded); (iii) amount of detail and experiments on the investigated topic. Hence, the selected results we analyze are strictly targeted to the following three aspects together (see Section 4.2): IoT, fog computing, and security/privacy. The peculiarities of guaranteeing security and privacy in fog environments will suddenly emerge, along with the outcomes obtained, until now, by the research community. Furthermore, in Section 4.3 we discuss ongoing EU projects and projects conducted outside the European Union, which fund research activities and partnerships in the fog computing field.

It is worth remarking that the selection process of review articles discussed in Section 2 does not strictly discard papers whose target is not centred on "IoT, fog computing, and security/privacy" because we also considered some results about edge computing, for example, in order to make a comparison with the presented work.

4.2. Security and privacy in IoT/fog computing environments

Firstly, we consider solutions that try to address authentication and authorization requirements. Inevitably, such approaches must consider the composition of the network architecture, since authorizations and credentials must be exchanged inside the running system. Fewer solutions are targeted to privacy or key management.

In this context, many solutions inspired by fog computing are related to smart health scenarios. For example, Moosavi et al. (2016) proposes an end-to-end security scheme for facilitating the mobility of medical sensors in a healthcare system, by means of smart gateways, which are interconnected among each other to compose the fog layer. More in detail, an end-user authentication and authorization architecture, based on the certificates and DTLS (Datagram Transport Layer Security) handshake is conceived; then, end-to-end communication security is obtained by means of mechanisms using session resumption. A full hardware/software prototype has been realized to demonstrate the feasibility of the presented approach, as well as the consequent improvement in energy consumption.

A similar solution is presented in Rahmani et al. (2018), which also exploits smart gateways for performing various tasks closer to healthcare sensors, such as local data processing, data filtering, data compression, data fusion, data analysis, adaptivity, local storage, local actuation. Security issues are only partially covered, referring to HTTPS protocol and on not well-defined cryptographic primitives. A proof-of-concept has been deployed to test the proposed architecture by providing node implementation, networked smart gateways implementation, and back-end and users' interface implementation.

The platform described in Thota et al. (2018) aims to secure authentication and authorization of involved healthcare devices, in order to: (i) identify and track the deployed devices; (ii) locate and track mobile devices; (iii) manage deployment and connection of new devices; (iv) allow communication among the devices and data transfer among remote healthcare systems. As the previous works Moosavi et al. (2016) Rahmani et al. (2018), also such a paper leverages the capabilities of DTLS to provide a security solution for the transport layer in the IoT environment (i.e., among the end-devices and the fog layer). Various well-known cryptography libraries such as symmetric keys, public keys, and hash algorithms, are then adopted for guaranteeing data integrity and confidentiality at the application layer.

Instead, Elmisery et al. (2016) mainly focuses on privacy principles in healthcare systems. A holistic framework is proposed for privacy management and enforcement, in compliance with the OECD (Organization for Economic Cooperation and Development) privacy principles. The authors propose to give all the control on privacy preferences to the end-users (i.e., the patients), which must declare their rules to be applied for their data treatment. The platform performs a sort of translation of such rules in privacy policies, which will be applied by the fog layer towards the cloud system.

Finally, with regards to the healthcare context, Manogaran et al. (2018), besides it provides no real implementation, presents an architecture for healthcare systems' monitoring and alerting systems, which adopts Meta Fog-Redirection (MF-R) and Grouping and Choosing (GC) architecture. The former uses big data technologies for the collection and storage of the data, generated from different sensors or devices. The latter is used for trying to secure the integration of fog computing with cloud computing; in fact, it uses a key management service and data categorization functions for guaranteeing end-to-end secure communications.

Another investigated application field is provided by the Internet of Vehicles (IoV). A trusted communication scheme among vehicles and a fog-computing infrastructure is presented in Arif et al. (2018). More in detail, a *fog anonymizer* (which is a sort of centralized and trusted third-party) acts as an intermediate among the vehicles and the location-based servers, and it is responsible for gathering and providing the required privacy level for each vehicle belonging to the network. Note that its activity mainly consists of blurring the information obtained from vehicles before sending them to the location-based servers.

Instead, the work in Kang et al. (2018) focuses on addressing location privacy issues, even in IoV environments. It reveals that, in traditional pseudonym systems, the pseudonym management is carried out by a centralized party (e.g., a cloud), resulting in big latency and high cost. Therefore, the authors suggest moving such a task towards the network edge, thus providing the following advantages: (i) context-aware pseudonym changing; (ii) timely pseudonym distribution; (iii) reduced pseudonym management overhead.

Dsouza et al. (2014) proposes a policy-based system for the management of resources in fog computing, expanding the current fog computing platform, in order to support secure collaboration and interoperability. A smart transportation system is considered as a use case to clarify the functionalities of the presented approach. Policies are expressed in XACML (eXtensible Access Control Markup Language) language. The policy management framework mainly consists of the traditional components, which are: PEP (Policy Enforcement Point), PDP (Policy Decision Point), and PAP (Policy Administration Point).

A cryptographic solution, which is based on a dynamic key-dependent approach, in order to allow for a good compromise between the security level and computational complexity, is presented in Noura et al. (2019). Some security tests have been carried out and include the randomness evaluation of the obtained data and the generated dynamic keys. In particular, the authors considered different statistical properties for performance evaluation, including randomness, correlation, independence, and uniformity. Also, a cryptanalysis discussion has been proposed, in order to validate the robustness of the conceived approach.

The literature also reveals solutions based on physical-based authentication. For example, face identification and resolution technology are adopted in a fog computing/IoT context in Hu et al. (2017b), in order to ensure the identity consistency of humans, saving bandwidth and improving processing capacity. Several security and privacy issues are discussed, such as: (i) the encryption of facial images in order to guarantee the data confidentiality during transmission and storage; (ii) the adoption of the mechanism of data integrity checking; (iii) the introduction of authentication and authorization mechanisms, with the support of session key agreement schemes, for verifying the identity validity of the networks' participants. The proposed mechanisms seem to be promising, as demonstrated by the results obtained from the development of the prototype system.

A physical framework based on fog computing and IoT is presented in Sehgal et al. (2015), whose target is smart human security. The IoT layer interacts with the physical world and gathers knowledge regarding the physical surroundings. It also takes elementary security decisions. The cloud and fog layers take more sophisticated decisions based on the complexity of situations and real-time requirements.

Furthermore, some works are focused on cyber-security frameworks and fog platforms, aimed at detecting attacks or at guaranteeing privacy. In this context, Sohal et al. (2018) envisions a cyber-security framework for identifying malicious edge devices in a fog computing environment; such a solution is essentially based on three technologies, which are: the Markov model, an intrusion

Table 3
Security and privacy requirements treated by works about fog computing in the IoT.

Requirement	Works
authentication, authorization, access control	Dsouza et al. (2014) Hu et al. (2017b) Moosavi et al. (2016) Rahmani et al. (2018) Sicari et al. (2017) Thota et al. (2018)
key management	Manogaran et al. (2018) Noura et al. (2019)
privacy	Elmisery et al. (2016) Kang et al. (2018) Lu et al. (2017)
security-aware architecture	Dsouza et al. (2014) Manogaran et al. (2018) Martin et al. (2017) Moosavi et al. (2016) Rahmani et al. (2018) Rizzardi et al. (2016) Sehgal et al. (2015) Sicari et al. (2017) S.Sicari et al. (2016) Thota et al. (2018)
secure end-to-end communications	Manogaran et al. (2018) Martin et al. (2017) Moosavi et al. (2016) Noura et al. (2019) Rahmani et al. (2018) Thota et al. (2018)
trust	Arif et al. (2018) Martin et al. (2017)
malicious devices' detection	Lu et al. (2017) Sohal et al. (2018) S.Sicari et al. (2016)
secure mobility	Moosavi et al. (2016)
monitoring and reporting	Ionita and Patriciu (2016) Manogaran et al. (2018) Martin et al. (2017)

detection system, and a virtual honeypot device. Note that edge devices' attacks could potentially become a bottleneck in the successful implementation and diffusion of fog computing environments, since the power-constrained IoT end-devices are very vulnerable due to their limited resources. Hence, new solutions must be conceived, in order to protect such devices both from internal and external attacks within the IoT network.

Again with the scope of detecting malicious behavior, the work in Ionita and Patriciu (2016) proposes the use of fog computing for enabling the efficient and real-time exchange of information about threats among different organizations. By sharing current attacks' information, the cyber-security field could benefit from the detection of up-to-date, sophisticated, and even orchestrated cyber-attacks, which could be put timely put in place, in order to minimize the damages that occurred when an attack is performed. To achieve such a goal, the fog computing layer should be equipped with a neural network.

A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT environments is proposed in Lu et al. (2017). Its aim is to early filter false data injected by external attackers, support fault tolerance, and efficiently aggregate hybrid IoT devices' data into one.

A distributed IoT platform, composed of several NOSs (NetwOrked Smart objects), is conceived in S.Sicari et al. (2016) to perform an automatic evaluation of security and data quality metrics on information coming from heterogeneous IoT devices, in real-time. Such an architecture has been further extended to support an authenticated publish/subscribe mechanism, based on the MQTT protocol (Rizzardi et al., 2016), in order to provide a more efficient data sharing with interested data consumers. Then, NOSs have been integrated with a sticky policy enforcement framework, in order to move data access control towards the edge of the network (Sicari et al., 2017), in a fog computing fashion, but a real fog layer is not deployed yet.

Finally, an architecture originally based on fog computing principles is OpenFog (Martin et al., 2017). The paper limits to point out how such a platform should be integrated with new security modules and functions, which should provide: (i) physical security of the fog nodes; (ii) end-to-end security within the device-fog-cloud continuum; (iii) trustworthiness of user processes executing in the fog nodes; (iv) security monitoring and management among the hardware/software entities present in the device-fog-cloud continuum. Note that the paper does not refer to privacy requirements.

After such an overview, it is clear that such studies reveal some of the main topics of interest in the field of security and privacy in IoT/fog computing environment, which will be detailed in Section 5. They are sketched in Table 3, in relation to the respective works treating them. Note that an important feature turned out to be end-to-end security in data exchanges, which is fundamental to guarantee higher robustness to the system.

4.3. Ongoing projects

It is also important to have a look at the ongoing projects in the field of fog computing and IoT. Such topics are an object of interest by the European Commission. In the context of Horizon 2020, the mF2C (Fog-to-Cloud) proposal (mF2C project, 2C, 0000) sets the goal of designing an open, secure, decentralized, multi-stakeholder management framework, including novel programming models, privacy and security, data storage techniques, service creation, brokerage solutions, policies, and resource orchestration methods. IoT capabilities and the cloud, coupled with fog computing principles, should bring new business opportunities. Concerning security and privacy, the project aims to increase the trust in clouds, through stronger security and data protection practices, including open and verifiable solutions for data security. Moreover, it envisions an increase in the control by users of their data and trust relations, thanks to the pervasiveness of fog devices. PrEstoCloud project (Proactive Cloud Resources Management at the Edge for efficient Real-Time Big Data Processing) (PrEstoCloud project, 0000), also funded by the European Union's Horizon 2020 research and innovation program, aims to combine real-time big data, cloud computing and fog computing research in order to provide an innovative solution for cloud-based adaptive real-time big data processing. Security-related activities are focused on the definition of access permissions and constraints to access both fog and cloud resources. H2020 CHARIOT project (0000) is specifically targeted to solve security and privacy issues in cloud computing and IoT contexts by leveraging fog computing principles. More in detail, the proposed system architecture aims to address the issues related to safety-critical systems in a fog network made up of heterogeneous IoT devices and gateways. DITAS EU H2020 project (Data-intensive applications Improvement by moving daTA and computation in mixed cloud/fog environmentS) (DITAS project, 0000) proposes a novel approach for developing data-intensive applications based on Virtual Data Containers (VDC), which let the developers simply define the requirements and access policies on the needed data, expressed as data utility, and take the responsibility of providing these data timely, securely, and accurate by hiding the complex underlying infrastructure composed by different platforms, storage systems, and network capabilities. To this end, VDCs will implement data and computation strategies to decide where, when, and how to save data (i.e., on the cloud or at the edge of the network).

Beyond Europe, a project which involves the United States, China and Japan is the Industrial Internet Consortium (OpenFog Consortium, 0000), which aims to create an open reference architecture for fog computing, build operational models and test-beds, define and advance technology, educate the market and promote business development through an innovative OpenFog ecosystem. A wide range of requirements are analyzed within the mentioned project; concerning security and privacy, the focus is on the evaluation, classification, and recommendation of security standards, practices, and technologies, as described in Martin et al. (2017) (see Section 4.2).

Finally, DECENTER project (0000) is an H2020 European and South Korean research and innovation project aiming to deliver a robust fog computing platform, which will provide application-aware orchestration and provisioning of resources, driven by methods based on artificial intelligence. The underlying infrastructure will form a federation and will utilize blockchain and smart contracts to reach secure processing, automated operation and timely delivery of responses to the users' queries.

Summarizing, the adoption of fog computing to manage IoT data is of great interest to the research community, as demonstrated by the ongoing projects in such a field. Note that not only academia, but also industry participates in such projects, which take into account both architectural, interoperability and scalability challenges and security and privacy design issues.

5. Security and privacy challenges and future research directions

The security and privacy issues strictly depend on the kind of environment and network infrastructure to be designed. Concerning IoT and fog computing, the smart devices belonging to the "fog" layer of the network act as intermediaries between the end-users along with data sources, and the cloud. They are conceived as powerful devices, routers, or gateways, owning processing capabilities to be exploited to perform specific computing tasks, such as data elaboration or aggregation, algorithms' execution, and security tasks, as introduced in Section 3. Hence, fog nodes can be represented as proxies, which are also able to provide cryptographic computations; while the underlying IoT devices and sensors lack the necessary resources to do such tasks. Therefore, fog computing not only provides additional computational resources to the network, but also a further level of security that could help in preventing, minimizing, and also counteracting attacks in the IoT environments. Furthermore, the adoption of the fog computing paradigm could help in preserving the privacy of IoT data and in protecting users' sensitive information by reducing the need to transmit certain kinds of data to the cloud for the required analysis. The exploitation of fog computing also encourages performing the analysis and processing of the data at the network edge, closer to the IoT devices that generate and act on that data (Sen and Yamin, 2021).

However, such an approach introduces, in the authors' opinion, several challenges concerning data, location, and users' security and privacy. The following aspects deserve particular attention:

- Which encryption technique should be adopted in order to ensure end-to-end security from data acquisition by data producers and their reception to data consumers?
- How to regulate the access control and authentication of end-user devices or data sources with fog devices? And how to manage the access control and authentication of fog devices?
- How to protect the information related to devices' location?
- How to guarantee anonymization, privacy and trust along the whole data life-cycle?
- How to put in act an efficient key management system?
- It would be better to dispose of a hierarchic fog architecture, or it could be better to have a single fog computing-based layer?
- How to support policies' definition, update, and synchronization, even among different application realms?
- Is it possible to integrate a fog computing architecture with a policy enforcement framework, due to the wide area, which is normally involved in a typical fog/IoT environment?
- How to prevent and monitor internal and external attacks both to end-devices and to fog nodes? And, how is it possible to react against violation attempts, once recognized?
- How to put in act logging and reporting systems about the fog layer activities, in order to reveal anomalies?

Furthermore, the mobility of IoT and users' devices, which is typical in fog computing, also introduces further security and privacy issues into the fog network (Puliafito et al., 2017). Fog nodes, in fact, frequently join and leave the fog layer, in a very dynamic way. The following questions naturally emerge:

- How access control rules and security and privacy policies should be modified when a fog node joins or leaves the fog layer?
- How to manage the authentication of end-user devices or data sources towards newly joined fog nodes?
- How to manage encryption/decryption keys' update or revocation, in presence of cryptography algorithms?
- How to preserve the privacy of the end-user devices when a fog node leaves the fog layer?
- How to design and develop a lightweight authentication schema among end-users devices and fog nodes in the scalable and dynamic fog network?
- How to maintain the anonymity of the end-user devices once misbehavior is detected from a fog node by the cloud service provider?

In the following, we try to give a response to such questions and to highlight open issues and future research directions, starting from the security and privacy requirements pointed out in Section 2 and taking into account the solutions investigated in Section 4.2. As emerged in Section 4.2, existing solutions specifically targeted to security and privacy in IoT contexts adopting fog computing paradigm do not fully address the mentioned issues, but only partially cover some of them.

Data confidentiality and integrity - encryption mechanisms. First of all, as far as the encryption mechanisms are concerned, we point out that many solutions presented in Section 4.2 do not specify any technique to be used for ciphering the data or location information, in order to preserve their confidentiality and integrity. However, such a feature is a crucial requirement for protecting the whole data life cycle; in fact, information, in an IoT environment, is gathered by producers and, then, sent to the fog computing layer of the network, to be further shared with the interested consumers. Fig. 2 summarizes and clearly points out the possible ways and places to perform an attack in a fog computing and IoT infrastructure. As just revealed, during the information's transmission, data confidentiality or integrity may be violated by malicious entities; at the same time, data can also be violated when they are stored on fog nodes or in the cloud.

Besides the traditional encryption techniques (which suffer, in the IoT environment, of high computational costs), other solutions for guaranteeing such requirements could be related to the data format; in fact, in Huang et al. (2017a) the XML encryption standard is expanded to efficiently and securely filter multiple encrypted XML streams and perform aggregation operations without decryption in the fog nodes. Such a solution cannot only be applied to the scenario of XML data exchange for publish/subscribe service, but also provides a secure and privacy-preserving method for data protection. In IoT applications, JavaScript Simple Object Notation (JSON) is the most popular format, and JSON Web Encryption (JWE), which utilizes standard cryptographic algorithms, is the standard for encrypting JSON data. In the IoT, due to fact that the

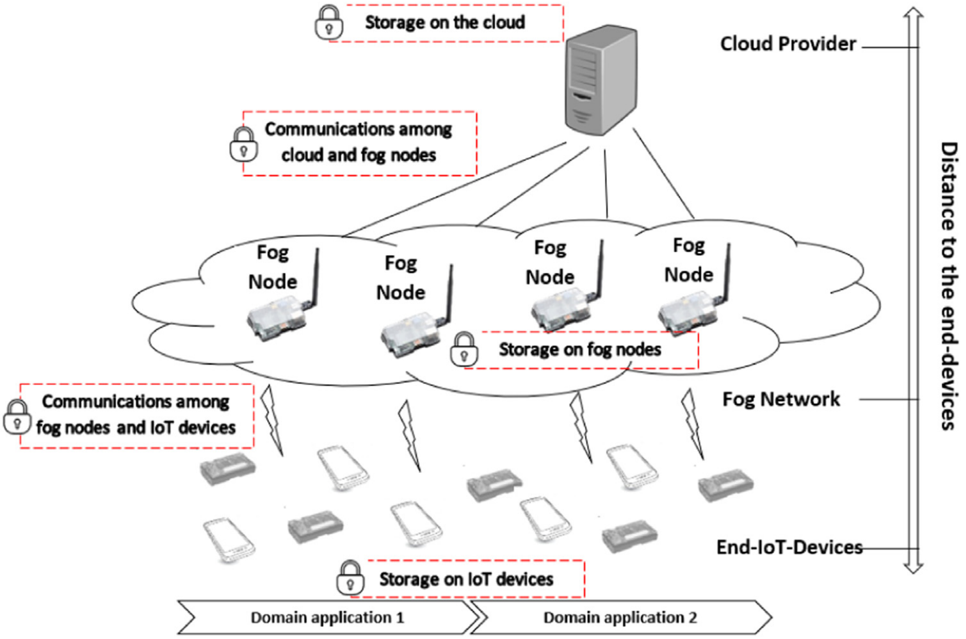

Fig. 2. IoT environment based on fog computing paradigm: possible threats.

most prevalent protocols are publish/subscribe protocols, such as Message Queue Telemetry Transport (MQTT) and Advanced Message Queuing Protocol (AMQP), fog computing should also adopt such a method for sharing data. A secure, fog computing-based, publish/subscribe lightweight protocol using Elliptic Curve Cryptography (ECC) for the IoT is proposed in Diro et al. (2017). It is worth remarking that ECC provides shorter key lengths, reduced message sizes and lower resource usages; if, at the same time, fog nodes offload some of computation and storage overheads from IoT nodes in proximity, then better scalability, and fewer overheads such as storage and communications, are provided with respect to RSA based schemes, employed in SSL/TSL, guaranteeing, at the same time, the same level of security.

Hence, the challenge we identified, with regards to the encryption mechanisms, is to choose or define a solution able to guarantee: (i) the required level of data protection, confidentiality, and integrity; (ii) lightweight operations to be performed on end-devices; (iii) distribution of tasks and synchronization among the fog nodes. Other related issues are the following: (i) how to manage entities' registration to the IoT system; (ii) how to store securely the devices' and users' credentials.

Key management. Besides the encryption techniques, which should take into account the possibility of dealing with power-constrained devices, also an efficient key management system should be designed, in order to guarantee that the encryption/decryption keys are protected against leakage or tampering. Concerning key management, several aspects should be defined, ranging from key distribution across different application realms and devices to key update and revocation in case of violation attempts or in case of policies' changes. These are open challenges in IoT/fog computing environment; mechanisms available in the literature for IoT technologies, such as WSN, can be considered as starting points to conceive new solutions targeted to fog computing (Roman et al., 2011) Sicari et al. (2016).

Access control. Note that the way of encrypting data also determines the policies for data disclosure. In other words, which users/devices are granted to access encrypted data? How access control is then performed? Due to its distributed nature, fog computing would facilitate the adoption of many standard access control models, such Attribute-Based Access Control (ABAC). For example, Attribute-Based Encryption (ABE) (Sahai and Waters, 2005) mechanisms allow to encrypt data for multiple recipients, in such a way that only those recipients whose attributes satisfy a given access policy can decrypt afterward. In a distributed architecture, we envision fog computing as an ideal candidate to grant access tokens to authorized parties who use them to perform a given action (e.g., data decryption). Also, a fog computing platform can be used as a sort of trust authority to authorize access and relay data among authorized parties and IoT devices. The solution detailed in Huang et al. (2017b) proposes to couple ABE and ABS (Attribute-Based Signature) techniques to guarantee a fine-grained data access control in an IoT infrastructure. Since ABE and ABS procedures have high costs in terms of processing, then fog computing is introduced; more in detail, the more complex ABE and ABS functions are delegated to the more powerful fog nodes, instead of power-constrained IoT devices. Instead, the authors of Alrawais et al. (2017b) propose a novel encrypted key exchange protocol based on CP-ABE (Bethencourt et al., 2007) for secure communications in a fog computing network. Also the works in Zuo et al. (2018) and Sicari et al. (2020) envision the adoption of ABE in fog computing. Such an approach is rapidly spreading due to its flexibility in terms of attributes' definition, which perfectly fits the heterogeneity of IoT environments. However, certain issues, mostly related to IoT/fog environments, such as key revocation management, computational needs, and multi-authority schemes, must be taken into account.

In our opinion, new solutions should enable and encourage the control of the data by the owners themselves, which should be provided with the necessary means for establishing, in an autonomous or semi-autonomous way, how to share their information. In such a direction, a feasible approach is that of sticky policies (Karjoth et al., 2002) Sicari et al. (2017). Sticky policies are transmitted along with the data they refer to throughout the entire data life cycle. The concept of sticky policy is to attach security and privacy policies to owners' data and drive access control decisions and policy enforcement. Sticky policies allow specifying access rules in an extremely fine-grained manner: in principle, every data unit could have its own, unique, policy. Furthermore, as policies 'travel' with the data across the entire system, they could protect the entire data life cycle. In this sense, sticky policies could help users to pursue their rights and actively manage the rules to be applied to their own information. In fact, if cloud-based systems would allow the users to provide not only the data, but also the associated policies, then the system and the third parties should only be equipped with the necessary software for respecting the defined policies. Such behavior represents a fundamental step for improving the trustworthiness of the cloud customers with respect to the actual service providers and for avoiding improper resource disclosure. Moving to a fog computing environment, such a task could be handled closer to the data producers and managed in a fine-grained way, lightening the cloud systems.

The challenge, in this case, is how to integrate the sticky policies within a fog computing architecture, considering that actual approaches, based on sticky policies, leverage make use of a trust authority to obtain access permission. Clearly, according to the distributed nature of the IoT context, multiple trust authorities could be adopted, and a synchronization mechanism among them could be integrated. Another kind of solution is the just mentioned ABE approaches, which always requires the presence of a trusted authority, but it not must be always online during the system's activities. However, one of the well-known limits of ABE techniques is that they can be more expensive, in terms of computation and storage, in presence of many attributes to be put in relation to define the policies themselves. To cope with such an issue, for example, the work proposed in Saidi et al. (2022), built on CP-ABE, presents *SHARE-ABE*, which is a novel collaborative approach, based on groups of users, for preserving privacy exploiting fog computing to outsource the most laborious decryption operations to fog nodes. They collaborate to partially decrypt the data using an original and efficient chained architecture. Additionally, such an approach preserves the privacy of the access policy by introducing false attributes. Another open issue is, besides the access control on data, how to guarantee the access control and authorization of end-devices and fog-devices themselves. Also, in this case, available solutions targeted to IoT could be revised to consider fog computing principles (Liu et al., 2012).

Finally, viable alternatives are those related to some international standards, such as *W3C Open Digital Rights Language (ODRL)*(ODRL, 0000), which is a policy expression language that provides a flexible and interoperable information model, vocabulary, and encoding mechanisms for representing statements about the usage of content and services. The ODRL information model defines the semantics of the ODRL policies, which are used to represent permitted and prohibited actions over a certain asset, as well as the obligations required to be met by stakeholders.

Anonymization and privacy. To provide anonymization techniques is another fundamental aspect for guaranteeing both data confidentiality and privacy. Traditional systems include k-anonymity, l-diversity, t-closeness (Li et al., 2007; Rajendran et al., 2017) and make use of techniques such as generalization, suppression, quasi-identifiers. Their main scope is to obfuscate or conceal sensitive information in order to control individuals' identifiability by third parties. In addition, the adoption of a suitable encryption scheme, as discussed above, would allow to efficiently transmit, in a ciphered way, both the data and, eventually, the policies. Some promising approaches have been cited and could represent relevant starting points for further investigations in the area. In the IoT/fog computing context, privacy-preserving techniques could be applied between the fog and the cloud to preserve data privacy because both have sufficient storage and power. It is challenging, though, to run such techniques between the fog layer and IoT devices, due to IoT resources' constraints. One possible solution is a privacy-preserving technique based on homomorphic functions (Li et al., 2010) that could be deployed to maintain the transmitted data's privacy. Differential privacy (Yin et al., 2018) is another technique to ensure the non-disclosure of privacy in the data-set. Therefore, techniques such as homomorphic encryption can be used to allow privacy-preserving aggregation at the local fog gateways without needing decryption. With regards to aggregation and statistical queries, differential privacy can be applied to ensure non-disclosure of privacy of an arbitrary single entry in the data-set. In such a way, security both during transmission and in storage is guaranteed. Nevertheless, the computational overhead of such approaches still represents an issue for constrained devices.

Another fundamental requirement is related to location privacy. With regards to location privacy preservation, one initial solution is to allow the IoT devices to distribute sensitive information about their location among several fog nodes, thus avoiding a single point of failure on a single fog node. Such a solution could waste fog resources and increase the delay time, since it requires a further effort for retrieving the information about location every time. Hence, such a solution would be viable to protect users' privacy only if an efficient privacy-preserving technique based on partitioning (Tu et al., 2010) the data among fog devices would be designed. To cope with such an issue, another solution may be adopted, which is based on an identity obfuscation technique (Ardagna et al., 2007). It can be used in the fog computing layer for IoT devices such that fog nodes cannot identify which IoT device is offloading the data. Hence, what emerges is that location is fundamental and easy-to-know information, which should be always available to allow efficient data processing and exchanges, but it should be also protected at the same time. The challenge is ever more critical due to devices' mobility, which could require a continuous update of such information.

Trust and rogue node detection. As emerged from the above discussion, some access control systems typically require the presence of a trusted party in order to manage access permissions to resources. Is it possible to envision a system in which parties are only partially trusted (e.g., honest-but-curious)? Or the end-devices must trust the fog nodes and, in turn, the fog nodes must trust the cloud systems? To cope with such issues, the authors in Alrawais et al. (2017a) propose the realization of a trust model, in IoT/fog environments, based on the continuous real-time evaluation of the reputation of the entities, taking part in the IoT environment. Such a technique can be applied to detect rogue nodes, when trust measurements are under a certain threshold. However, in the heterogeneous IoT context it is very difficult to set up proper rules and artificial intelligence mechanisms able to properly work. In Fortino et al. (2020), current architectures for modeling trust in IoT and fog environments are deeply investigated. Instead, the work in Farhadi et al. (2019) envisions the adoption of blockchain technology for guaranteeing data security in IoT/fog computing applications. Blockchain mechanisms could represent a revolution in such a field, despite computational costs must be taken into account; to cope with such an issue the approach proposed in Wu and Ansari (2020) adopts a cooperative computing strategy to mitigate and reduce computing power consumption. Note that solutions addressing the trust and reputation challenge probably have a low impact in the short term, but could significantly boost the chances of IoT and fog computing being adopted at scale in the long term, mainly in contexts that usually treat high sensitive information (Yan et al., 2014).

Monitoring, logging, reporting and attack detection. Monitoring, logging, and reporting represent crucial requirements for any security system, in order to detect attacks and check the ability of the system to behave as expected in response to certain situations. In the case of fog computing, such monitoring should extend to the complete data life-cycle and the whole IoT network. Such an aspect represents a distinctive feature with respect to traditional monitoring and detection solutions, which usually involve a more limited area. Moreover, unlike the cloud servers, fog nodes may be vulnerable to physical attacks, since they are closer to the end-users. To ensure end-to-end security, it is also essential to protect fog nodes against hardware tampering or electromagnetic eavesdropping. Another fundamental concern is that most IoT devices and fog nodes are usually remotely managed. Remote management offers opportunities for adversaries to conduct various network-based attacks, and makes the detection and mitigation of these attacks more difficult and costly. In a fog computing-based network, some monitoring, logging, and reporting tasks on IoT devices can be delegated to the fog nodes; however, also the behavior of the fog nodes should be controlled, since they are not considered trusty.

In such a scenario, the main challenge is related to the fact that new threats, vulnerabilities, or even simple changes in the environment, may lead to the emergence of new attack vectors. Thus, an efficient monitoring and reporting system would quickly respond to the changes in the security landscape, thus preventing or suddenly reacting to incoming attacks. Enabling logging and telemetry collection on the fog nodes represent essential requirements in such a direction, to increase situational awareness and contextual awareness. Moreover, support from an events' analysis engine is also expected, in order to correctly correlate the events and changes occurring in the IoT context. Recognized issues will trigger proper notifications for allowing the system to promptly react to violations and threats. Also, the attack's propagation should be inhibited. Such challenges are often overlooked in the realization of IoT systems, and require more attention by designers and developers.

It is worth remarking that, when a new solution, protocol, or method is designed, it should be tested before real deployment. Hence, the availability of simulation environments specifically targeted to fog computing becomes urgent. Until now, the most popular existing toolkit for modeling and simulating the resource management techniques and protocols of fog computing is *iFogSim* (Gupta et al., 2017).

6. Conclusion

The fog computing-based approaches showed many advantages to overcome scalability and interoperability issues in the IoT era, where more and more devices are connected in the real world, thus generating a huge amount of data to be processed and shared. The spreading of fog computing design solutions is even more encouraged by the diffusion of IoT applications, such as smart cities, smart buildings, smart transport, smart health, and so on, but also by the increasing adoption of 5G connectivity. The paper has presented various facets of security and privacy requirements, issues, and challenges in the IoT context, adopting fog computing. Concerning security and privacy in the fog layer, insights have been provided on available solutions, also pointing out open challenges and hints for future research directions. Some aspects of security and privacy-preserving solutions are more mature than others, such as access control and encryption mechanisms; while other ones deserve more attention in the next future, such as key management, location privacy, trust models, and monitoring systems to foster attack detection and prevention. We do hope that the discussion we provided can be of interest to various audiences, including most notably Ph.D. candidates, research consortia, and the IT industry, in order to pursue the realization of secure and privacy-aware, efficient IoT-based fog computing infrastructures.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Abbadi, I., Martin, A., 2011. Trust in the cloud . Information Security technical report 16 (3–4), 108 –114.
Alli, A.A., Alam, M.M., 2020. The fog cloud of things: a survey on concepts, architecture, standards, tools, and applications. Internet of Things 9, 100177.
Alrawais, A., Alhothaily, A., Hu, C., Cheng, X., 2017. Fog computing for the internet of things: security and privacy issues. IEEE Internet Comput 21 (2), 34–42.
Alrawais, A., Alhothaily, A., Hu, C., Xing, X., Cheng, X., 2017. An attribute-based encryption scheme to secure fog communications. IEEE Access 5, 9131–9138.
Ardagna, C.A., Cremonini, M., Damiani, E., Di Vimercati, S.D.C., Samarati, P., 2007. Location privacy protection through obfuscation-based techniques. In: IFIP Annual Conference on Data and Applications Security and Privacy. Springer, pp. 47–60.
Arif, M., Wang, G., Balas, V.E., 2018. Secure vanets: trusted communication scheme between vehicles and infrastructure based on fog computing. Stud. Inform. Control 27 (2), 235–246.
Atayero, A.A., Feyisetan, O., 2011. Security issues in cloud computing: the potentials of homomorphic encryption. Journal of Emerging Trends in Computing and Information Sciences 2 (10), 546–552.
Avasalcai, C., Murturi, I., Dustdar, S., 2020. Edge and fog: a survey, use cases, and future challenges. Fog Computing: Theory and Practice 43–65.
Bethencourt, J., Sahai, A., Waters, B., 2007. Ciphertext-policy attribute-based encryption. In: Security and Privacy, 2007. SP'07. IEEE Symposium on, pp. 321–334.
Bonomi, F., Milito, R., Zhu, J., Addepalli, S., 2012. Fog computing and its role in the internet of things. In: Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing. ACM, pp. 13–16.
Butun, I., Sari, A., Österberg, P., 2019. Security implications of fog computing on the internet of things. In: 2019 IEEE International Conference on Consumer Electronics (ICCE). IEEE, pp. 1–6.
CHARIOT project. https://www.chariotproject.eu. Online, accessed 2022.
Chen, N., Chen, Y., Song, S., Huang, C.-T., Ye, X., 2016. Smart urban surveillance using fog computing. In: Edge Computing (SEC), IEEE/ACM Symposium on. IEEE, pp. 95–96.
Constant, N., Borthakur, D., Abtahi, M., Dubey, H., Mankodiya, K., 2017. Fog-assisted wiot: a smart fog gateway for end-to-end analytics in wearable internet of things. arXiv preprint arXiv:1701.08680.
Costa, B., Bachiega Jr, J., de Carvalho, L.R., Araujo, A.P., 2022. Orchestration in fog computing: a comprehensive survey. ACM Computing Surveys (CSUR) 55 (2), 1–34.
DECENTER project. https://www.decenter-project.eu. Online, accessed 2022.
Dillon, T., Wu, C., Chang, E., 2010. Cloud computing: issues and challenges. In: Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on. IEEE, pp. 27–33.
Diro, A.A., Chilamkurti, N., Kumar, N., 2017. Lightweight cybersecurity schemes using elliptic curve cryptography in publish-subscribe fog computing. Mobile Networks and Applications 22 (5), 848–858.
DITAS project. https://www.ditas-project.eu., Online, accessed 2022.
Dsouza, C., Ahn, G.-J., Taguinod, M., 2014. Policy-driven security management for fog computing: Preliminary framework and a case study. In: Information Reuse and Integration (IRI), 2014 IEEE 15th International Conference on. IEEE, pp. 16–23.
Dubey, H., Yang, J., Constant, N., Amiri, A.M., Yang, Q., Makodiya, K., 2015. Fog data: Enhancing telehealth big data through fog computing. In: Proceedings of the ASE BigData & SocialInformatics 2015. ACM, p. 14.
Elmisery, A.M., Rho, S., Botvich, D., 2016. A fog based middleware for automated compliance with oecd privacy principles in internet of healthcare things. IEEE Access 4, 8418–8441.
Fahmideh, M., Zowghi, D., 2020. An exploration of IoT platform development. Inf Syst 87, 101409.
Farhadi, M., Miorandi, D., Pierre, G., 2019. Blockchain enabled fog structure to provide data security in IoT applications. arXiv preprint arXiv:1901.04830.
Fernandes, D.A., Soares, L.F., Gomes, J.V., Freire, M.M., Inácio, P.R., 2014. Security issues in cloud environments: a survey . Int. J. Inf. Secur. 13 (2), 113–170.
Fortino, G., Fotia, L., Messina, F., Rosaci, D., Sarné, G.M., 2020. Trust and reputation in the internet of things: state-of-the-art and research challenges. IEEE Access 8, 60117–60125.
Gia, T.N., Jiang, M., Rahmani, A.-M., Westerlund, T., Liljeberg, P., Tenhunen, H., 2015. Fog computing in healthcare internet of things: A case study on ECG feature extraction. In: Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on. IEEE, pp. 356–363.
Gupta, H., Vahid Dastjerdi, A., Ghosh, S.K., Buyya, R., 2017. Ifogsim: a toolkit for modeling and simulation of resource management techniques in the internet of things, edge and fog computing environments. Software: Practice and Experience 47 (9), 1275–1296.
Habibi, P., Farhoudi, M., Kazemian, S., Khorsandi, S., Leon-Garcia, A., 2020. Fog computing: a comprehensive architectural survey. IEEE Access 8, 69105–69133.
Hu, P., Dhelim, S., Ning, H., Qiu, T., 2017. Survey on fog computing: architecture, key technologies, applications and open issues. Journal of Network and Computer Applications 98, 27–42.
Hu, P., Ning, H., Qiu, T., Song, H., Wang, Y., Yao, X., 2017. Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things . IEEE Internet Things J. 4 (5), 1143–1155.
Huang, J.-Y., Hong, W.-C., Tsai, P.-S., Liao, I.-E., 2017. A model for aggregation and filtering on encrypted xml streams in fog computing . Int. J. Distrib. Sens. Netw. 13 (5).

Huang, Q., Yang, Y., Wang, L., 2017. Secure data access control with ciphertext update and computation outsourcing in fog computing for internet of things. IEEE Access 5, 12941–12950.

Ionita, M.-G., Patriciu, V.-V., 2016. Secure threat information exchange across the internet of things for cyber defense in a fog computing environment. Informatica Economica 20 (3).

Kang, J., Yu, R., Huang, X., Zhang, Y., 2018. Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles. IEEE Trans. Intell. Transp. Syst. 19 (8), 2627–2637.

Karjoth, G., Schunter, M., Waidner, M., 2002. Privacy-enabled services for enterprises. In: Database and Expert Systems Applications, 2002. Proceedings. 13th International Workshop on. IEEE, pp. 483–487.

Khalid, T., Abbasi, M.A.K., Zuraiz, M., Khan, A.N., Ali, M., Ahmad, R.W., Rodrigues, J.J., Aslam, M., 2021. A survey on privacy and access control schemes in fog computing . Int. J. Comm un. Syst. 34 (2), e4181.

Khan, S., Parkinson, S., Qin, Y., 2017. Fog computing security: a review of current applications and security solutions. Journal of Cloud Computing 6 (1), 19.

Kitanov, S., Monteiro, E., Janevski, T., 2016. 5g and the fog - survey of related technologies and research directions. In: Electrotechnical Conference (MELECON), 2016 18th Mediterranean. IEEE, pp. 1–6.

Laroui, M., Nour, B., Moungla, H., Cherif, M.A., Afifi, H., Guizani, M., 2021. Edge and fog computing for iot: a su rvey on current research activities & future directions. Comput Commun 180, 210–231.

Lee, J.Y., Lee, J., 2021. Current research trends in iot security: a systematic mapping study. Mobile Information Systems 2021.

Lee, K., Kim, D., Ha, D., Rajput, U., Oh, H., 2015. On security and privacy issues of fog computing supported internet of things environment. In: Network of the Future (NOF), 2015 6th International Conference on the. IEEE, pp. 1–3.

Lee, W., Nam, K., Roh, H.-G., Kim, S.-H., 2016. A gateway based fog computing architecture for wireless sensors and actuator networks. In: Advanced Communication Technology (ICACT), 2016 18th International Conference on. IEEE, pp. 210–213.

Li, F., Luo, B., Liu, P., 2010. Secure information aggregation for smart grids using homomorphic encryption. In: Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on. IEEE, pp. 327–332.

Li, G., Wu, J., Li, J., Wang, K., Ye, T., 2018. Service popularity-based smart resources partitioning for fog computing-enabled industrial internet of things . IEEE Trans. Ind. Inf. 14 (10), 4702–4711.

Li, J., Jin, J., Yuan, D., Palaniswami, M., Moessner, K., 2015. Ehopes: Data-centered fog platform for smart living. In: Telecommunication Networks and Applications Conference (ITNAC), 2015 International. IEEE, pp. 308–313.

Li, N., Li, T., Venkatasubramanian, S., 2007. t-closeness: Privacy beyond k-anonymity and l-diversity. In: 2007 IEEE 23rd International Conference on Data Engineering, pp. 106–115.

Li, S., Da Xu, L., Zhao, S., 2018. 5G internet of things: a survey. Journal of Industr ial Information Integration.

Liu, J., Xiao, Y., Chen, C.P., 2012. Authentication and access control in the internet of things. In: Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on. IEEE, pp. 588–592.

Lu, R., Heung, K., Lashkari, A.H., Ghorbani, A.A., 2017. A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. IEEE Access 5, 3302–3312.

Luan, T.H., Gao, L., Li, Z., Xiang, Y., Wei, G., Sun, L., 2015. Fog computing: focusing on mobile u sers at the edge. arXiv preprint arXiv:1502.01815.

Mahmud, R., Kotagiri, R., Buyya, R., 2018. Fog computing: a Taxonomy, survey and fu ture directions. In: Internet of Everything. Springer, pp. 103–130.

Manogaran, G., Varatharajan, R., Lopez, D., Kumar, P.M., Sundarasekar, R., Thota, C., 2018. A new architecture of internet of things and big data ecosystem for secured smart healthcare monitoring and alerting system. Future Generation Computer Systems 82, 375–387.

Martin, B.A., Michaud, F., Banks, D., Mosenia, A., Zolfonoon, R., Irwan, S., Schrecker, S., Zao, J.K., 2017. Openfog security requirements and approaches. In: Fog World Congress (FWC), 2017 IEEE. IEEE, pp. 1–6.

Martinez, I., Hafid, A.S., Jarray, A., 2020. Design, resource management, and evaluation of fog computing systems: a survey . IEEE Internet Things J. 8 (4), 2494–2516.

mF2C project, 2C. https://www.mf2c-project.eu/tag/fog-computing., Online, accessed 2022.

Miorandi, D., Rizzardi, A., Pellegrini, F.D., Chlamtac, I., 2012. Internet of things: vision, a pplications and research challenges. Ad Hoc Netw 10, 1497–1516.

Moosavi, S.R., Gia, T.N., Nigussie, E., Rahmani, A.M., Virtanen, S., Tenhunen, H., Isoaho, J., 2016. End-to-end security scheme for mobility enabled healthcare internet of things. Future Generation Computer Systems 64, 108–124.

Mostafavi, S., Shafik, W., 2019. Fog computing architectures, privacy and security solutions. Journal of Communications Technology, Electronics and Computer Science 24, 1–14.

Mouradian, C., Naboulsi, D., Yangui, S., Glitho, R.H., Morrow, M.J., Polakos, P.A., 2017. A comprehensive survey on fog computing: state-of-th e-art and research challenges. IEEE Communications Surveys & Tutorials 20 (1), 416–464.

Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M.A., Choudhury, N., Kumar, V., 2017. Security and privacy in fo g computing: challenges. IEEE Access 5, 19293–19304.

Munir, A., Kansakar, P., Khan, S.U., 2017. Ifciot: integrated fog cloud iot: a novel ar chitectural paradigm for the future internet of things. IEEE Consum. Electron. Mag. 6 (3), 74–82.

Naranjo, P.G.V., Pooranian, Z., Shojafar, M., Conti, M., Buyya, R., 2018. Focan: a fog–supported smart city network archite cture for management of applications in the internet of everything environments. J Parallel Distrib Comput.

Ni, J., Zhang, K., Lin, X., Shen, X.S., 2017. Securing fog computing for internet of things applic ations: challenges and solutions. IEEE Communications Surveys & Tutorials 20 (1), 601–628.

Noura, H., Salman, O., Chehab, A., Couturier, R., 2019. Preserving data security in distributed fog computing . Ad Hoc Netw 9 4, 101937.

ODRL. https://www.w3.org/TR/odrl-model/., Online, accessed 2022.

OpenFog Consortium. https://www.iiconsortium.org/index.htm., Online, accessed 2022.

Okay, F.Y., Ozdemir, S., 2016. A fog computing based smart grid model. In: Networks, Computers and Communications (ISNCC), 2016 International Symposium on. IEEE, pp. 1–6.

PrEstoCloud project. http://prestocloud-project.eu., Online, accessed 2022.

Puliafito, C., Mingozzi, E., Anastasi, G., 2017. Fog computing for the internet of mobile things: issues and challenges. In: Smart Computing (SMARTCOMP), 2017 IEEE International Conference on. IEEE, pp. 1–6.

Puliafito, C., Mingozzi, E., Longo, F., Puliafito, A., Rana, O., 2019. Fog computing for the internet of things: a survey. ACM Tr ansactions on Internet Technology (TOIT) 19 (2), 1–41.

Rahmani, A.M., Gia, T.N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M., Liljeberg, P., 2018. Exploiting smart e-health gateways at the edge of healthcare internet-of-things: a fog computing approach. Future Generation Computer Systems 78, 641–658.

Rajendran, K., Jayabalan, M., Rana, M.E., 2017. A study on k-anonymity, l-diversity, and t-closeness techniques. IJCSNS 17 (12), 172.

Rejiba, Z., Masip-Bruin, X., Marín-Tordera, E., 2019. A survey on mobility-induced service migration in the fog, edge, and related computing paradigms. ACM Computing Surveys (CSUR) 52 (5), 1–33.

Rizzardi, A., Sicari, S., Miorandi, D., Coen-Porisini, A., 2016. AUPS: An open source authenti cated publish/subscribe system for the internet of things. Inf Syst 62, 29–41.

Roman, R., Alcaraz, C., Lopez, J., Sklavos, N., 2011. Key management systems for sensor networks in the context of the internet of things. Computers & Electrical Engineering 37 (2), 147–159.

Roman, R., Lopez, J., Mambo, M., 2018. Mobile edge computing, fog et al.: a survey an d analysis of security threats and challenges. Future Generation Computer Systems 78, 680–698.

Román-Castro, R., López, J., Gritzalis, S., 2018. Evolution and trends in iot security . Computer (L ong Beach Calif) 51 (7), 16–25.

Sahai, A., Waters, B., 2005. Fuzzy identity-based encryption. In: Eurocrypt, Vol. 3494. Springer, pp. 457–473.

Saidi, A., Nouali, O., Amira, A., 2022. Share-abe: an efficient and secure data sharing framework based on ciphertext-policy attribute-based encryption and fog computing . Cluster Compu t 25 (1), 167–185.

Salman, O., Elhajji, I., Chehab, A., Kayssi, A., 2018. IoT survey: an SDN an d fog computing perspective. Comput. Networks.

Sehgal, V.K., Patrick, A., Soni, A., Rajput, L., 2015. Smart human security framework using internet of things, cloud and fog computing . In: Intelligent Distributed Computing. Springer, pp. 251–263 .

Sen, A.A.A., Yamin, M., 2021. Advantages of using fog in iot applications. International Journal of Information Technology 13 (3), 829–837.

Sha, K., Yang, T.A., Wei, W., Davari, S., 2020. A survey of edge computing-based designs for IoT security. Digital Communications and Networks 6 (2), 195–202.

Sicari, S., Rizzardi, A., Dini, G., Perazzo, P., La Manna, M., Coen-Porisini, A., 2020. Attribute-based encryption and sticky policies for data access control in a smart home scenario: a comparison on networked smart object middleware . Int. J. Inf. Secur. 1–19.

Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A., 2015. Security, privacy and trust i n internet of things: the road ahead. Comput. Networks 76, 146–164.

Sicari, S., Rizzardi, A., Miorandi, D., Coen-Porisini, A., 2016. Internet of Things: security in the keys. In: 12th ACM International Symposium on QoS and Security for Wireless and Mobile Networks, pp. 129–133. Malta

Sicari, S., Rizzardi, A., Miorandi, D., Coen-Porisini, A., 2017. Security towards the edge: st icky policy enforcement for networked smart objects. Inf Syst 71, 78–89.

Singh, S., Jeong, Y.-S., Park, J.H., 2016. A survey on cloud computing security: issues, threats, a nd solutions. Journal of Network and Computer Applications 75, 200–222.

Sohal, A.S., Sandhu, R., Sood, S.K., Chang, V., 2018. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Computers & Security 74, 340–354.

Sookhak, M., Yu, F.R., He, Y., Talebian, H., Safa, N.S., Zhao, N., Khan, M.K., Kumar, N., 2017. Fog vehicular computing: augmentation of fog computing using vehicular cloud computing. IEEE Veh. Technol. Mag. 12 (3), 55–64.

S.Sicari, Rizzardi, A., Miorandi, D., Cappiello, C., Coen-Porisini, A., 2016. A secure and quality-aware pr ototypical architecture for the internet of things. Inf Syst 58, 43–55.

Stantchev, V., Barnawi, A., Ghulam, S., Schubert, J., Tamm, G., 2015. Smart items, fog and cloud computing as enablers of servitization in healthcare. Sensors & Transducers 185 (2), 121.

Stojmenovic, I., Wen, S., 2014. The fog computing paradigm: Scenarios and security issues. In: Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on. IEEE, pp. 1–8.

Tang, B., Chen, Z., Hefferman, G., Wei, T., He, H., Yang, Q., 2015. A hierarchical distributed fog computing architecture for big data analysis in smart cities. In: Proceedings of the ASE BigData & SocialInformatics 2015. ACM, p. 28.

Thota, C., Sundarasekar, R., Manogaran, G., Varatharajan, R., Priyan, M., 2018. Centralized fog computing security platform for IoT and cloud in healthcare system. In: Ex ploring the Convergence of Big Data and the Internet of Things. IGI Global, pp. 141–154.

Truong, N.B., Lee, G.M., Ghamri-Doudane, Y., 2015. Software defined networking-based vehicular adhoc network with fog computing. In: Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on. IEEE, pp. 1202–1207.

Tu, M., Li, P., Yen, I.-L., Thuraisingham, B.M., Khan, L., 2010. Secure data objects replication in data grid . IEEE Trans Dependable Secure Comput 7 (1), 50–64.

Vaquero, L.M., Rodero-Merino, L., 2014. Finding your way in the fog: towards a comprehensive definition of fog computing. ACM SIGCOMM Computer Communication Review 44 (5), 27–32.

Wen, Z., Yang, R., Garraghan, P., Lin, T., Xu, J., Rovatsos, M., 2017. Fog orchestration for iot services: issues, challenges and directions . IEEE Intern et Comput 21 (2), 16–24.

Wu, D., Ansari, N., 2020. A cooperative computing strategy for blockchain-secured fog computing . IEEE Internet Things J. 7 (7), 6603–6609.

Wu, D., Liu, S., Zhang, L., Terpenny, J., Gao, R.X., Kurfess, T., Guzzo, J.A., 2017. A fog computing-based framework for process monitoring and prognosis in cyber-manufacturing . J. Manuf. Syst. 43, 25–34.

Yan, Z., Zhang, P., Vasilakos, A.V., 2014. A survey on trust management for internet of things. Journal of network and computer applications 42, 120–134.

Yi, S., Li, C., Li, Q., 2015. A survey of fog computing: concepts, applications and issues. In: Proceedings of the 2015 Workshop on Mobile Big Data. ACM, pp. 37–42.

Yi, S., Qin, Z., Li, Q., 2015. Security and privacy issues of fog computing: A survey. In: International Conference on Wireless Algorithms, Systems, and Applications. Springer, pp. 685–695.

Yin, C., Xi, J., Sun, R., Wang, J., 2018. Location privacy protection based on differential privacy strategy for big data in industrial internet of things . IEEE Trans. Ind . Inf. 14 (8), 3628–3636.

Zao, J.K., Gan, T.T., You, C.K., Méndez, S.J.R., Chung, C.E., Te Wang, Y., Mullen, T., Jung, T.P., 2014. Augmented brain computer interaction based on fog computing and linked data. In: Intelligent Environments (IE), 2014 International Conference on. IEEE, pp. 374–377.

Zuo, C., Shao, J., Wei, G., Xie, M., Ji, M., 2018. CCA-secure abe with outsourced decryption for fog computing. Future Generation Computer Systems 78, 730–738.

Sabrina Sicari is an Associate Professor at the University of Insubria (Varese). She received a degree in Electronical Engineering, 110/110 cum laude, from the University of Catania, in 2002, where in 2006 she got Ph.D. in Computer and Telecommunications Engineering, followed by Prof. Aurelio La Corte. She is a member of COMNET, IEEE IoT, ETT, ITL editorial board. Her research activity security, privacy, and trust in WSN, WMSN, IoT, and distributed systems.

Alessandra Rizzardi is an Assistant Professor in Software Engineer at the University of Insubria (Varese). She received BS/MS degree in Computer Science 110/110 cum laude at the University of Insubria, in 2011/2013. In 2016 she got Ph.D. in Computer Science and Computational Mathematics at the same university, under the guidance of Prof. Sabrina Sicari. Her research activity is on WSN and IoT security issues.

Alberto Coen Porisini received Dr. Eng. degree and Ph.D. in Computer Engineering from Politecnico di Milano in 1987 and 1992. He is a Professor of Software Engineering at Universit degli Studi dell'Insubria since 2001, Dean of the School of Science since 2006 and Dean since 2012. His research regards the specification/design of real-time systems, privacy models, and WSN.