Computer Science Review 41 (2021) 100421

Contents lists available at ScienceDirect

Computer Science Review

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

Review article

Security in fog computing: A systematic review on issues, challenges and solutions

Ronita Rezapour [a], Parvaneh Asghari [b,*], Hamid Haj Seyyed Javadi [c], Shamsollah Ghanbari [d]

[a] Department of Computer Engineering, Islamic Azad University Qom Branch, Qom, Iran
[b] Department of Computer Engineering, Islamic Azad University Central Tehran Branch, Tehran, Iran
[c] Department of Mathematics and Computer Science, Shahed University, Tehran, Iran
[d] Department of Computer Engineering, Islamic Azad University Ashtian Branch, Ashtian, Iran

ARTICLE INFO

Article history:
Received 17 August 2020
Received in revised form 18 June 2021
Accepted 5 August 2021
Available online xxxx

Keywords:
Fog computing
Cloud computing
Security in fog computing

ABSTRACT

Fog computing refers to cloud computing development to the edge of a corporate network. Fog computing, as a promising computing paradigm, facilitates computing, storing and network services between terminal devices and cloud computing data centers. It also brings many advantages to cloud computing and large-scale deployment of IoT applications such as low latency, data locality, location-awareness, mobility, less computational cost and geographical distribution. This extensive range of functionality raises various security concerns related to data, virtualization, segregation, network communication and monitoring. Security is a significant issue for fog computing since fog-based services are offered to massive-scale end-users by front fog nodes/servers. Also, fog computing focuses on ensuring the availability and reliability of services without worrying about the information stored or processed by the fog. Despite significant efforts that have been made in this field, many issues are still open. This paper prepares a comprehensive study of security challenges and different approaches in fog computing to address those challenges using the Systematic Literature Review (SLR) approach. Moreover, a technical taxonomy is offered for the fog security challenges and their strategies in terms of six aspects, including reliability, access control, attacks, secure connection, privacy and some special cases. The core objective of this study is to analytically and statistically classify the existing research techniques related to security aspects and available solutions in fog computing published between 2014 and 2021. Then some technical questions in this domain are provided, and also the strengths and weaknesses of each indicated fog security approach are discussed based on the questions, as well as suggesting some ideas to address security deficiencies in fog computing. Finally, some future motivational directions and open issues in this field are provided to design, implement, and maintain fog systems.

Contents

* Corresponding author.
E-mail address: p_asghari@iauctb.ac.ir (P. Asghari).

https://doi.org/10.1016/j.cosrev.2021.100421
1574-0137/© 2021 Elsevier Inc. All rights reserved.

1. Introduction

Fog computing is a platform introduced by Cisco with the purpose to extend the cloud capabilities closer to the edge of the network [1]. The term "fog" simply issued because "fog is a cloud close to ground", i.e. From cOre to edGe computing, enabling refined and better applications [2]. Fog computing is a geographically distributed computing architecture connected to multiple heterogeneous devices at the edge of the network, but at the same time not exclusively seamlessly backed by cloud services. Hence, we envisage fog as a bridge between the cloud and the edge of the network that points to aid in developing of the recently emerging IoT applications [1].

Cloud computing as a novel technology has transformed the macro world. It has led to the on-demand availability of various services with shared resources to be conceivable on the internet [2]. Cloud service providers (CSPs) enlarge applications and services in the cloud, and users can utilize the presented highly available and effective computing resources with low cost from a shared resource pool (network, servers, storages, applications, services, etc.) pay-as-you-go basis [3]. In other words, to encounter the huge amount of data processing, cloud computing is considered as a fascinating option while preparing a cost-effective solution with sufficient storing and computing resources in cloud data centers [4].

Simultaneously, with the expansion of cloud computing and the explosive growth of IoT technologies, the number of specified applications that are used in different fields, including security, safety, cost-saving, asset tracking, agriculture, smart metering, smart cities, and smart homes, has increased. The IoT has significantly modified the quality of human life through the environment wherein smart services are given to utilize in daily lives. All these conveniences and services are supplied through the different applications carried out in the IoT environment management [5,6]. IoT equipment generates a lot of data, putting a lot of pressure on the communications infrastructure and the internet. Cloud helps store, process, and transfer data to IoT equipment instead of local devices. For instance, when an IoT device uses several sensors to collect data, each of these sensors requires a large amount of computation. This operation requires a lot of energy as well as cost. Under these conditions, data can be transferred to the cloud and processed there. IoT devices generally require fast processing and access to resources that limit the benefits of using the cloud in all cases. [7,8].

Although cloud computing makes our life more prosperous and efficient, with the exists issues of enlarging data transportation, deficiency of the data bandwidth, high latency and low mobility support, the expansion of using cloud computing, enhances these limitations that hinder the widespread adoptions of these novel techniques. Furthermore, other issues such as location awareness, centralized data storage and data processing, large response time latency, network congestion, and communication cost are yet substantial unsolved [3]. This has led to the emergence of fog technology. Cloud computing is a distributed infrastructure where data, computing and storage are located between data generators (IoT equipment) and the cloud. Using fog reduces data sent to the cloud, shortens response times for device requests, reduces security risks by storing data close to their location, and increasing mobility [7]. On the other side, fog computing, as a promising computing paradigm, is an extended and advanced prescription of cloud computing. Fog computing appears as a useful alternative to maintain geographically distributed, latency-sensitive, and QoS-aware IoT applications. Also, fog performs as a middle layer between the IoT objects and the cloud data centers. Its distributed approach also addresses constraints met by cloud computing through accomplishing most of the application processing using their resource. At the same time, the rest is diverted towards the cloud data center [2].

Fog computing paradigm provides innumerable benefits like reducing communication delay during a client's request and a cloud service provider's response time, decreasing network congestion, equipping devices with the abilities of computation at the fog nodes, lessening computational cost at the cloud server and many more other conveniences. Therefore, fog computing has led the cloud computing paradigm to be much more prosperous to handle or service [2]. Fog computing technology presents the possibility of implementing the cloud near the equipment, which generates the data and works on it. The equipment used in this implementation is called fog node, and it can be used everywhere through network connection [9,10]. Every device with three capabilities of computing, storing, sending and receiving the information through a network duct is capable of changing into a fog node. Some challenges of designing a fog computing system are as follows:

- Delay time [11,12].
- Network bandwidth allocation policies [11,13].
- Trust and fault tolerance [11,14].
- Collection and protection of data in different conditions such as geographical conditions, environmental limitations and so on [11].
- Selection of the best resource for processing, saving and transferring data [11,15].
- Security in fog computing technology [11,16].

The requirements for analyzing security in every environment are considered by three factors as follow which may change somewhat according to the domain they are used in [17].

- Confidentiality: preventing information disclosure to unauthorized people [18–20].
- Accessibility: the information must be accessible whenever authorized people need it [18,21]. The definition of accessibility in terms of the target community in an accessible security channel is different from the exact definition when data is storing and recovering [17].
- Integrity: preventing data alteration in unauthorized access and recognizing the modification of information manipulated in an unauthorized manner [18,22].

Previous research articles carried out a comprehensive classification of fog security issues and the benefits of fog computing and its unique characteristics [23,24]. In some other review studies, the details of the attacks [15] and additional security-related issues like security applications and secure sharing technology used in these classifications were discussed appropriately [25]. Some research articles revised fog based applications in smart cities regarding their security and privacy concerns [26]. Other papers surveyed on utilizing user behavior profiling and decoy technology to relieve security issues in fog computing [27], and some studies reviewed the ML (Machine Learning) functionalities in a fog computing environment [28]. However, due to the advent of new technologies and expansion of the combined applications of fog in a variety of contexts, regarding the increase of security risks, a different approach is necessary to classify the assortment of previous research articles in this field of knowledge. Furthermore, the varying and transforming security challenges in fog have conducted to generate new questions in these fields, which have led to the need for a comprehensive review study in an SLR form in this domain. The main contributions of this review study are as follows:

- Presenting an SLR method for analyzing the main security challenges in fog.
- Providing a technical taxonomy to classify the reviewing fog security based on six challenges of reliability, access control, attacks, secure connection, privacy and exceptional cases.
- Expressing some technical questions about the differences between fog computing and cloud computing's scope, fog computing's security challenges, its strengths and weaknesses also, representing future trends and possible solutions about security fog issues.
- Discussing and analyzing the approaches for solving the issues according to the gained answers to the provided technical questions.
- Proposing some future motivational trends and open issues in this field.

This review paper is structured as follows: In Section 2, the background, including the fog scope and its architecture, are presented. Section 3 surveys the existing related works. Section 4 provides a methodology to find and aggregate researches related to fog security challenges using a systematic approach and expressing some technical questions. Section 5 demonstrates the security challenges in fog computing and categorizes them through a technical taxonomy. Moreover, this section analyzes all studies conducted regarding the considered issues and compares them. In Section 6, technical questions about security in fog are discussed. Section 7 introduces general visions imaginable about the future of security issues in fog computing, and the conclusions are presented in Section 8.

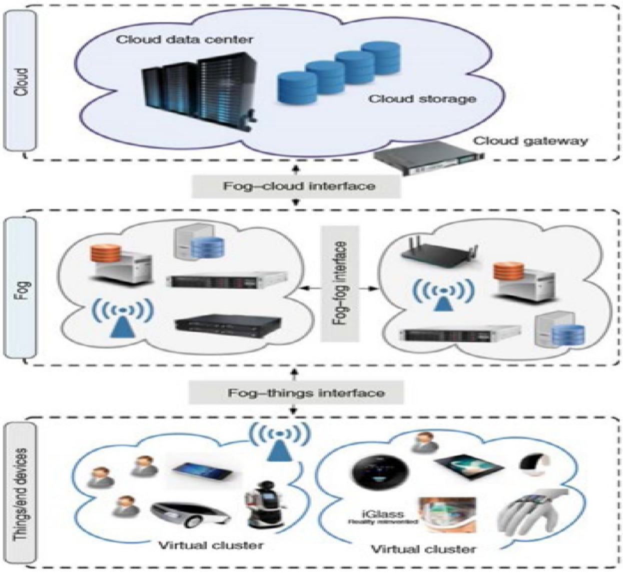

Fig. 1. Architecture of three-tier model of fog [4].

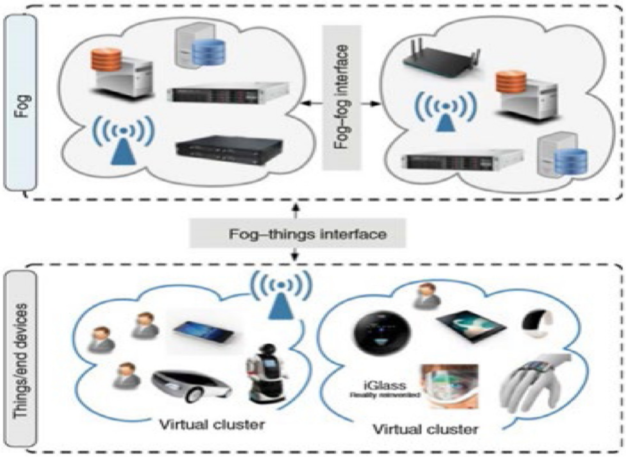

Fig. 2. Architecture of two-tier model of fog [4].

2. Background

This section presents the required concepts in fog computing and the requirements to acquire security concept in this area.

2.1. Architectures in fog

Fog networks give a distributed computing system with a hierarchical layout. Fog networks aim at considering precise timing, energy consumption reduction of base devices, presenting real-time data processing, local processing resource control and reducing backhaul traffic load to focused data center [29,30]. Fog computing has two different forms of architectures: (I) Cloud–Fog-Device architecture and (II) Fog-Device architecture [31]. Fig. 1 illustrates the three-tier model as the Cloud–Fog-Device architecture [32], and Fig. 2 displays the two-tier model as the Fog-Device architecture.

(I) *Cloud–Fog-Device architecture* comprises three tiers: cloud, fog computing and device. Generally, the device tier consists of two kinds of devices: mobile and fixed devices [33]. Fog tier includes network equipment with routers, gateways, bridges, switches and base devices with computing capability, including local servers. Each of these devices is considered a fog node. In three-tier architecture, the cloud tier is a storage and computing platform. The cloud has considerable storage capacity and computing resources, and it is accessible for users everywhere. Also, in this architecture, fog acts as a bridge between the computing resources available in the cloud and the data generating resources located in the devises tier and processing and storing [33].

(II) *Fog-Device architecture* as two-tier architecture consists of fog computing tier and device tier. In this architecture, fog nodes give different services in a coordinated way and without cloud servers' interferences. In contrast, in Cloud–Fog-Device architecture, fog nodes send data summary periodically according to internal hierarchical structure to the cloud after processing and analyzing collected data by IoT devices. In two-tier architecture, fog is responsible for processing data at the edge, storing and transmitting information from the data generating by mobile or fixed devices located in the devices tier [32,34].

The connection among tiers is provided through different connection technologies; wired connection (Ethernet, optical fiber), wireless connection (ZigBee, Bluetooth, NFC, IEEE 802.11 a/b/c/g/n and satellite links) or a compound of both [32].

The primary profit of the three-tier architecture is well-managing services. The services that are sensitive to delay are confronted with fog nodes that are situated near the end-users. Similarly, data gathering, data filtration and data clearing-related activities have to be carried out previously the data is delivered to the leading network, after that, enforcing the intermediate fog in the architecture. Besides, location-sensitive and privacy-aware services also necessitate different kinds of data and information to be fulfilled locally, in place of directing the data to the core network. This also intensifies the significance of three-tier architecture [4].

Due to fog nodes nature which is heterogeneous and distributed in different locations such as core, edge, access networks, and endpoints, it is essential to have proper fog resource management to provide flawless resource management through multiple platforms. Furthermore, the fog architecture should be flexible enough to host various applications such as vehicular networks and IoT applications [35]. In various usages, fog tire was deployed in the N-tire model, which makes several hierarchical fog deployment models. The N-tire model usually is proposed for diverse usages. Different hierarchical fog deployment models (N-tier fog deployment) for diverse uses in fog computing was presented in Fig. 3. (a) Without any fog collaboration; (b) Fog node collaboration; (c) Multi-tier(say, N-tier)fog node deployment; and (d) Global and local fog hierarchy [4].

2.2. Fog computing scope

In this section, two close concepts of fog computing, namely cloud and edge computing, are compared to aim at determining the extent and idea of fog computing briefly. Table 1, explains a comparison between cloud computing and fog computing in terms of some parameters such as delay, real-time support, mobility, awareness of the place, number of serving nodes, geographical distribution, distance to service recipients, service location, the necessary environment for activity, communication model, dependence on the quality of the central network, bandwidth consumption, ability to compute and store and energy consumption [36–39].

Also, Table 2 compares fog computing and edge computing in terms of some parameters such as architecture, delay, bandwidth consumption, access to resources, ability to compute and store, mobility ability, scalability, how to allocate services, data collection, processing, storage, IoT manages multiple programs simultaneously, competition for resources and focus [9,40–42].

3. Related work

In this section, the existing review and relevant papers published between 2014 and 2021 that covered security issues in fog computing are discussed and analyzed.

Fog computing utilizes one or more collaborative end-users or near-user edge devices to carry out storage, communication, control, configuration, optimization and management operations. Latency and bandwidth restriction issues met by utilizing cloud computing can be well solved using fog computing. First, Zhang, et al. [43] examined and analyzed the architectures of fog computing and demonstrated the relevant security and trust subjects. They comprehensively detailed how such subjects have been handled within the current literature. To conclude, they outlined the open challenges, research future directions to security and trust matters in fog computing.

Table 1
Comparing fog computing and cloud computing.

Compared parameters	Cloud computing	Fog computing
Delay	• Enormous	• Low
Real-time support	• Support-backing	• Support-backing
Mobility	• Low	• High
Awareness of the place	• Partially	• Full support
Number of Serving Nodes	• Low	• High
Geographical Distribution	• Centralized	• Decentralized
Distance to service recipients	• Usually high	• Usually low
Service location	• Internet	• At the edge of the local network
The necessary environment for activity	• Data storage centers that have an air conditioning system	• Anywhere
Communication model	• IP	• Wired (no limit)
Dependence on the quality of the central network	• High	• Low
Bandwidth consumption	• High	• Low
Ability to compute and store	• High	• Low
Energy consumption	• High	• Low

Table 2
Comparing fog computing and edge computing.

Compared parameters	Edge computing	Fog computing
Architecture	• Hierarchical • Decentralized • Distributed	• Hierarchical • Decentralized • Distributed
Distance to service recipients	• In the service provider's device	• Near the service recipient
Delay	• Low	• Low
Bandwidth consumption	• Low	• Low
Access to resources	• Very limited	• Limited
Ability to compute and store	• Limited	• Low
Mobility ability	• Support	• Support
Scalability	• Enormous	• Enormous
How to allocate services	• Virtual	• Virtual
Data collection, processing, storage	• Device • Edge of local network	• Network devices • Local area networks • Adjacent network devices
IoT manages multiple programs simultaneously	• Lack of support	• Support
Competition for resources	• High	• Low
Focus	• Level of objects	• Infrastructure level

Devices in IoT are interconnected and can exchange data with other connected devices. IoT environment can be expressed from distinctive points of view. Other than indicating IoT as a network for interplay between devices [44–46], in some fog based researches, this intercommunication has been categorized according to industry [47] and home [48] based implementation environment. Besides, Wireless Sensors and Actuators Network [49], Cyber–Physical Systems [50], Embedded system network [51], etc., have also been observed as diverse types of IoT while developing system and service models for fog computing.

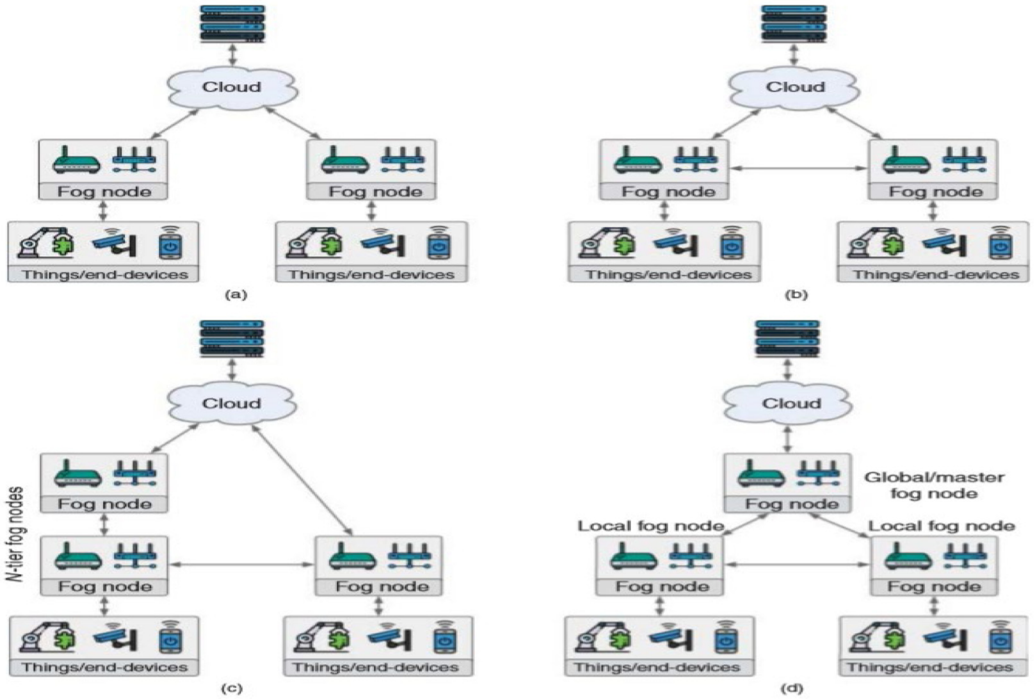

Fig. 3. Hierarchical fog deployment models (including N-tier fog deployment) [4].

In IoT healthcare platforms, monitoring is a key mechanism. Gia, et al. [52] provided a fog-based monitoring at a low cost. In addition, the platform includes smart gateways and productive IoT sensors. Moreover, sensors gather electrocardiography signals, body temperature, and breathe rate and send them wirelessly to gateways to deliver notices taking after an automated evaluation. Ahmad, et al. [53] proposed a fog-based healthcare platform, according to the content of privacy and security as key contents of existing health care platforms, where developed as a fog layer within the cloud and end devices by applying a modular approach. A cloud access security broker (CASB) was employed to increase privacy and security concerns at the network's edge. Also, data gathering [54] from various origins well can be upheld by the platform and satisfactory cryptographic evaluation. Healthcare information that is sensitive to delay seems to influence the efficiency of healthcare platforms.

Chakraborty, et al. [55] examined a fog-based computation framework to tackle delay-sensitive healthcare data about the time between the occurrence of an event and its handling. The large-scale geo-distributed healthcare framework was equipped with an application so that data consistency and data accuracy can be preserved and service delivery time can be leveraged. Monteiro, et al. [56] designed a fog based architecture to legislate and assess sensed rare health data. Embedded computing instances with limited resources were employed to identify the significant patterns and send them to the cloud. The essential purpose of this framework is to handle massive data through decreased power fog resources. A smart health gateway as a tool was designed by Negash, et al. and Rahmani, et al. [57,58] in fog computing to provide healthcare services in IoT and to supply data processing, data assessment, and real-time local storage. To provide reliable services, the smart e-health gateways were distributed geographically. Every gateway is obligated to perform the duty of controlling a group of IoT devices that are straightforwardly associated with the patient. This framework can screen patients regardless of their mobility. In this fog-based framework, energy-, mobility-, and reliability-related concerns can be settled successfully.

The smart city is a fascinating aspect that has made many researchers interested because of its comprehensive and immense effect on human's lives. A general revise based on a systematic literature review of available studies that have been accomplished in the field of fog based applications in smart cities with regards to its security and privacy concerns was presented by Javadzadeh, et al. [26]. Moreover, a preferable analytical match of peer works, the approaches, and the latter researches attitude were indicated in this article.

Almobaideen, et al. [27] reviewed current security approaches that utilize technologies like user behavior profiling and decoy technology to relieve security concerns in fog computing and other environments. Decoy data, such as decoy documents, honey pots and other bogus information, can be produced on demand and utilized to recognize unauthorized access to information and poison the thief's ex-filtrated information. Serving decoys will confound an attacker into conceiving they have ex-filtrated useful information when they have not. A summary of the users' characteristic and behavior patterns is produced and kept for future estimation. The Decoy technology can be combined with user behavior profiling technology to secure the user's data in fog and thereby to aid in recognition of invalid access. It prepares prevention to enable the proper distribution of data. Some classifications were offered in detecting unauthorized access and decoy technology deployment.

A review of the ML (Machine Learning) functionalities in a fog computing environment were presented by Abdulkareem, et al. [28]. The fog-based ML application gets a powerful end-user and a high service layer to catch more significant analytical smart responses to the required activities. A completed revise was proposed to highlight the last progress in ML approaches that are related to three issues of fog computing: managing of resource, accuracy, and security. Besides, other outlooks relevant to the ML domain, like kinds of application support, approaches, and dataset, were prepared.

In [16], Lee, et al. combined an explore sensor, a fog node and the cloud to unify a fog environment. They also described security concerns in each area. Fog computing prepares highly efficient service to the user by rectifying deficiency of cloud in IoT environment. IoT technology used in different fields should be protected from security threats. The necessity to prepare the secure fog computing environment via security technologies is also highlighted. A comprehensive effort could aim to implement a system to effectively gather and evaluate different logs produced in a fog computing environment. It prepares an important situation information for users.

Mahmud, et al. [59] reviewed recent implementations in fog computing. Challenges in fog computing were considered in terms of structural, service and security-relevant subjects. According to the specific major challenges and characteristics, a classification in fog environment has been proffered. The classification categorizes and analyzes the available researches according to their strategies for addressing the challenges. Besides, according to the evaluation, some motivating research trends proposed.

A fog computing paradigm expands cloud computing and services to the edge of the networks while offloading the cloud data centers and reducing service delivery time and response time to the end-users. However, the features of fog computing arise new security and privacy issues. The available cloud computing's security and privacy solutions cannot be straightly employed in fog computing because of its characteristics, such as mobility, heterogeneity, and large-scale geo-distribution. Mukherjee, et al. [23] reviewed current security and privacy concerns in fog computing and summarized them. After that, this highlighted ongoing research attempt, open issues, and research directions related to privacy and security challenges in fog computing.

Wang, et al. [24] proposed and considered the new concerns in fog security within an extended survey on the benefits of fog computing and its inimitable characteristics, matching diverse scenarios between fog computing and cloud computing. The outcome of this study will persuade more extended research on the fascinating field of fog security and fog forensics.

In [60] Zhang, et al. discussed and analyzed the fog computing architectures and indicated the relevant possible security and trust concerns. Then, how such concerns have been handled in the present research was extensively mentioned. In the end, the open issues, research directions and future security- and trust-relevant concerns in fog computing were considered.

Papers covered security issues and features in fog computing were summarized in Table 3.

4. Research selection method

This section illustrates all selected studies from 2014 to 2021 conducted about fog security using the SLR method. By including substitutes and equivalent words of the critical basic terms, this exploration string was appointed [5,40,43,60–63]: Fog computing; Cloud computing; Security in fog computing.

This systematic review provides the following technical questions, which will be responded to in Section 6:

- Q1: What are the differences between the scope of fog computing and cloud computing, and how fog computing can help to improve the current challenges in cloud computing?
- Q2: What are the security-related challenges in fog computing?
- Q3: What are the current solutions to fog computing security challenges and their strengths and weaknesses?
- Q4: What general vision is imaginable about the future of security in fog computing, and what new solutions can be proposed?

Table 3
The summary of review studies on security issues in fog computing.

References	Issue in fog	Feature
Lee, et al., 2015 [16]	• Fog environments • Data protection • MITM attack • Intrusion detection • Malicious detection method • Malicious fog node matter • Data management concerns	• Various security threats to the fog.
Mukherjee, et al., 2017 [23]	• Communications in the fog • Trust issue • Authentication • Malicious attacks	• Survey fog challenges
Wang, et al., 2015 [24]	• Trust issue • Dependability for data acquisition • Multi-tenancy issues • Chain of custody • Logs-related issues	• Fog security and fog forensics review
Zhang, et al. [43]	• Trust issue • Access control • Authentication	• Fog potential security and trust subjects
Gia, et al., 2017, Ahmad, et al., 2016 Chakraborty, et al., 2016, Monteiro, et al., 2016, Negash, et al., 2018 Rahmani, et al., 2018 [52,53,55–58]	• Privacy • Trust issue • Data consistency • Sensitive data latency • Service delivery time • handling massive data with constrained fog resources • Distributed fog nodes • Energy consumption • Network usage • Reliable services • Mobility • Authentication	• Fog-based healthcare framework
Javadzadeh, et al., [26] 2020	• Smart cities application • Security • Privacy • Mobility • Latency	• Survey on smart cities fog based applications
Almobaideen, et al. [27], 2020	• Security • Behavior profiling • Decoy technology • Authorization	• Review on current security approaches in fog
Abdulkareem, et al., 2019 [28]	• Managing of resource • Data Accuracy • Security	• Survey on issues' of using ML(Machine Learning) functionality in fog
Mahmud et al., 2018 [59]	• Privacy • Authentication • DoS attack • Encryption	• Reliability in the fog
Zhang et al., 2018 [60]	• Reliability • Authentication • Attack • Privacy • Connection	• Survey trust and security

Fig. 4 shows the distribution of the research articles over time based on their publishers, which were reviewed and cited in research such as IEEE, Elsevier, Springer, ACM, Wiley and Taylor & Francis. Also, some electronic databases such as Science Direct and IEEE Xplorer are employed.

After expressing the technical questions, we exert the admission criteria for the ultimate research selection. Considering the number of published studies, we just evaluated the journal

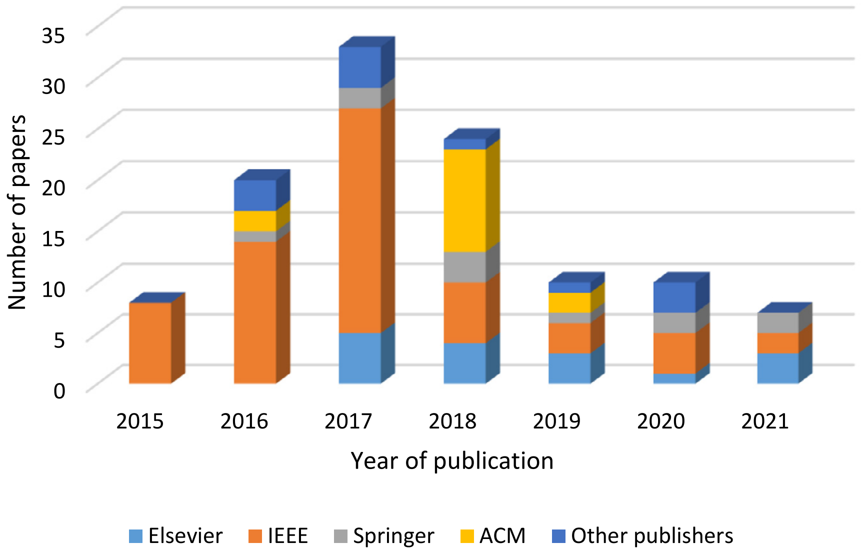

Fig. 4. Distribution of research articles by publisher.

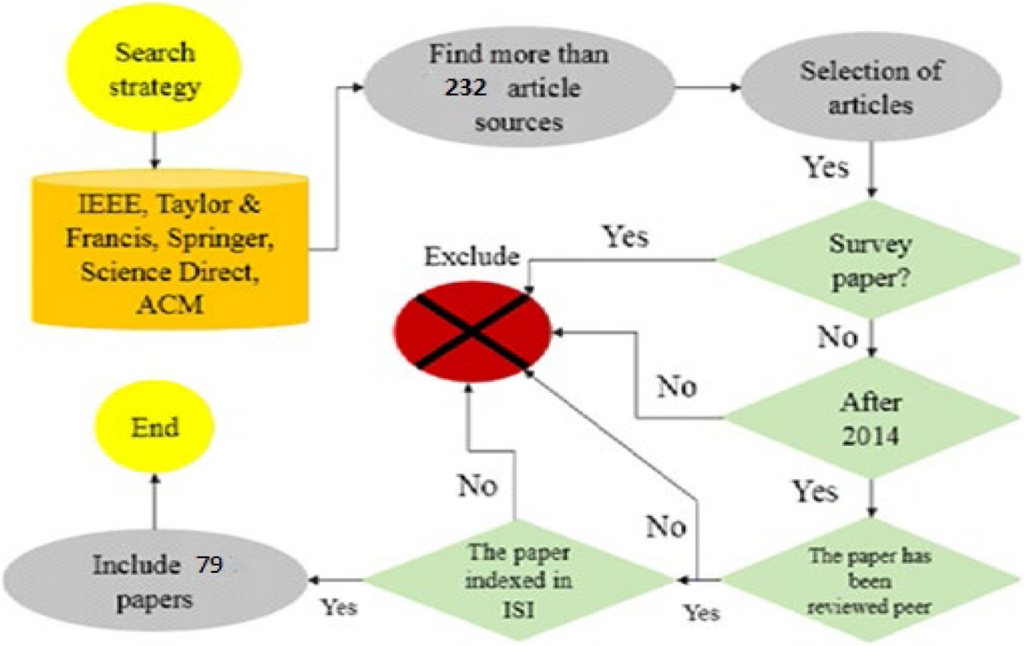

Fig. 5. Assessment criteria and framework of research papers.

articles and conference papers that indexed in ISI proceedings significant and associated papers for security challenges in fog. Finally, the 79 associated papers were supposed for further analysis to respond to our technical questions that are detailed in Section 4. The research method and article selection are presented in Fig. 5.

5. Security in fog computing and its challenges

In this section, all selected researches are analyzed, and the set of researchers' opinions in fog are classified. Based on reviewing the chosen articles, fog computing security issues are categorized via six approaches:

1. *Reliability*: regarding the approach that fog nodes can perform certain activities without any security problems and give the results to the stakeholders [59].
2. *Authentication and access control*: regarding the approach whether an entity (node, person, process) can access the resources or not [64,65].
3. Analyzing attacks: attacks' features, vulnerabilities and intrusion detection in fog [64,66,67].
4. *Analyzing privacy*: issues related to privacy with four approaches of personal privacy, data privacy, user privacy and situation privacy [65,68].
5. *Secure connection*: analyzing the problems and challenges in both internal and external relationships between fog nodes and other parts of fog environment, especially the internal network nodes [68].
6. *Other cases*: including service accessibility, security applications and secure sharing technology [69].

Fig. 6 explains the provided taxonomy of the security challenges in fog computing according to the context of the existing studies

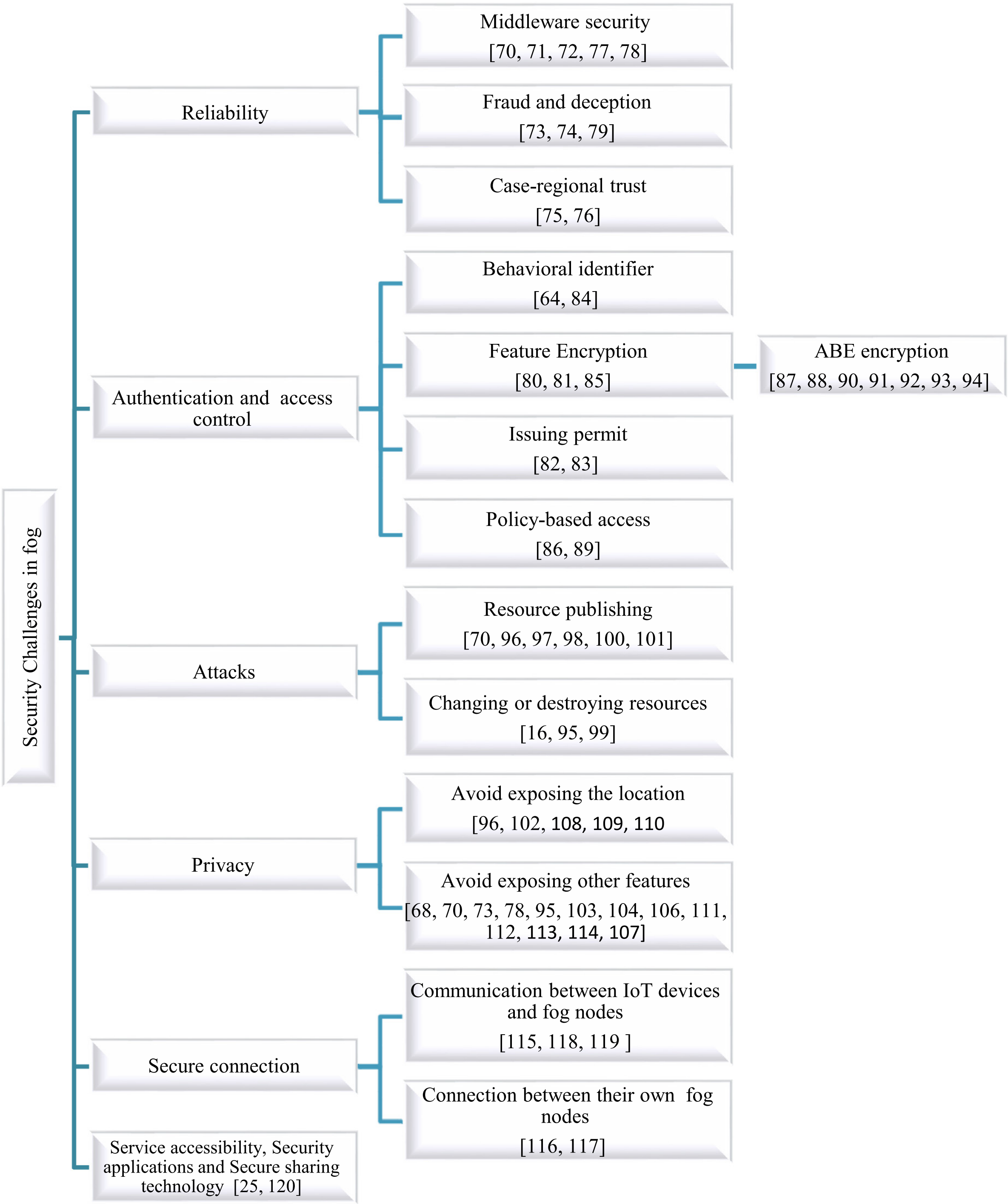
Security Challenges in fog
Reliability
Middleware security [70, 71, 72, 77, 78]
Fraud and deception [73, 74, 79]
Case-regional trust [75, 76]
Authentication and access control
Behavioral identifier [64, 84]
Feature Encryption [80, 81, 85]
ABE encryption [87, 88, 90, 91, 92, 93, 94]
Issuing permit [82, 83]
Policy-based access [86, 89]
Attacks
Resource publishing [70, 96, 97, 98, 100, 101]
Changing or destroying resources [16, 95, 99]
Privacy
Avoid exposing the location [96, 102, 108, 109, 110
Avoid exposing other features [68, 70, 73, 78, 95, 103, 104, 106, 111, 112, 113, 114, 107]
Secure connection
Communication between IoT devices and fog nodes [115, 118, 119]
Connection between their own fog nodes [116, 117]
Service accessibility, Security applications and Secure sharing technology [25, 120]

Fig. 6. The taxonomy of important security challenges in fog.

chosen based on the method illustrated in Section 4. The different groups of this taxonomy are described in detail in the following subsections.

According to the existing taxonomy, Fig. 7 presents a graph to show the following classification of all studies conducted about security in fog computing based on the released year.

5.1. Reliability

Reliability in researches emphasized the following aspects:

- Middleware security and giving some models for it [70].
- Analyzing collusion deception possibility [70].
- Region-based trust [70].

In [70], a middleware was proposed to optimize the reliability of connection between cloud and fog nodes. This middleware will determine reliability rate in the form of a hidden factor and analyzing connection packages.

A middleware in [71] was suggested to calculate nodes' reliability rate in cloud and fog connection based on maximum entropy.

In [72], the available trust model based on a middleware was divided into two general parts: security center, which is the most secure node of a local network, issues and analyzes

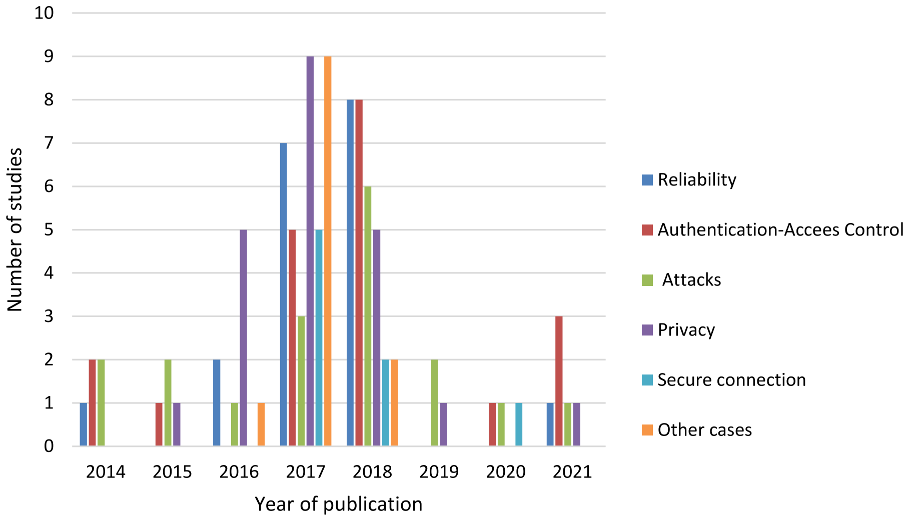

Fig. 7. The number of studies conducted about security in fog computing based on publication year.

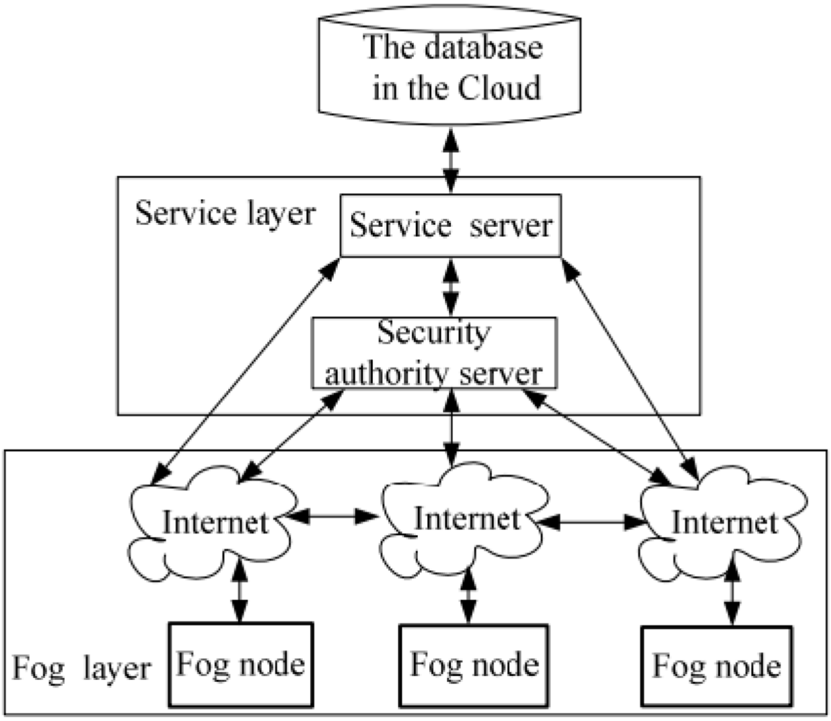

Fig. 8. Fog middleware trust model [70].

the security certificates; service server that has the capability of connecting fog internal and external layers. Fig. 8 shows the relations between middleware and other parts of the trust model.

Publish–Subscribe System was provided in [73] for confronting collision attacks. This system is displayed with the abbreviation PSS. PSS is widely used in crisis management systems as a supervisor of traffic and transport. The first plan using this reliability system developed based on preventing collusion can be observed in [74].

In [74], a broker is the essential part of a PSS (Preserving Publish/Subscribe) system. The requests are sent to brokers, and the connection is made between two pieces of a fog system or between a fog and a cloud system by a broker.

In [75], a model was developed for connection and trust development between fog nodes in different regions of the fog network. The access level structure of this region-based trust system can be observed in Fig. 9.

In this model, a node with the task of analyzing security in a region will be determined. This node is representative of managing computing resources and performing the functions in a region. The policy of selecting representative node according to the regional conditions and the delegated task to fog will be determined.

The way this method works was simply explained in Fig. 9. Node2 of region1 and node4 of region2 are representative nodes. If node3 wants to gain partial trust for connection, it must send the request to node2 to acquire trust and receive the required trust certificate from node [75].

In [76], a vehicular fog service (VFS) prepared by a vehicular fog (VF) was proposed, which is organized by integrating calculating and storing resources of stopped vehicles. VF dynamicity

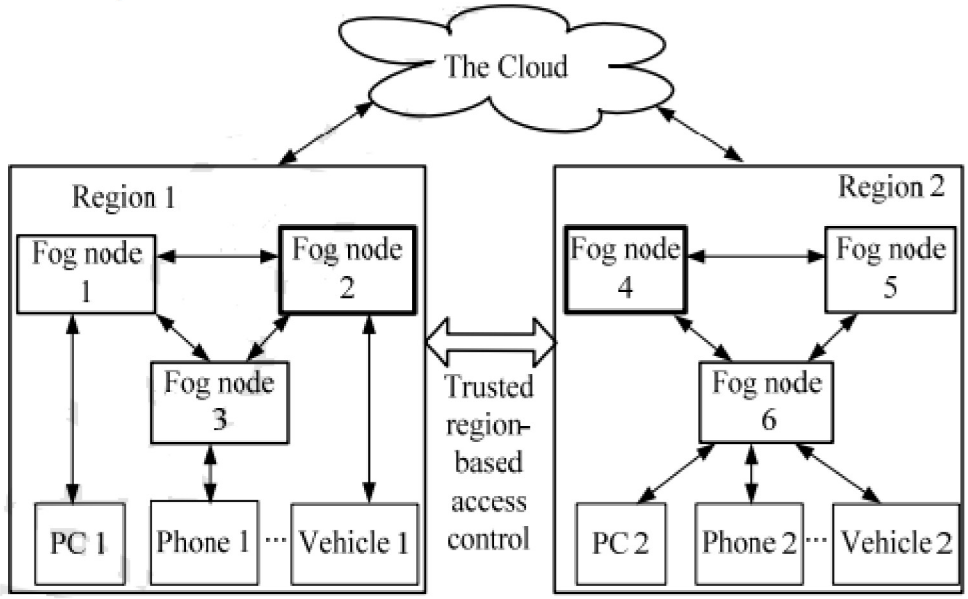

Fig. 9. The overview of region-based trust for fog [75].

causes issues in trusting and securing VFS prepared for client vehicles due to vehicles' unexpected arrivals and departures. A new structure was proposed, which comprises a VF construction strategy and a VFS access strategy to guarantee VFS reliability and security without sacrificing performance. The trustworthiness and security of VFS in this structure were examined in detail. Additionally, the effect of that structure on VF throughput was discussed, and it appeared that the construction is lightweight enough to utilize within the VFSs, which are sensitive to latency.

In [77], a solution to improve safe storage was proposed. The offered hybrid secure deduplication protocol merges client-side and server-side deduplication considering untrustworthy fog storage environments. The client-side deduplication is adopted in inter-network (i.e., cloud fog network) correlations to prevent network traffic flow at the network core. in contrast, the server-side deduplication is applied in intra-network (i.e., user-fog network) correlations to prohibit information leakage through side channels to improve data privacy. The result of the evaluation indicates the comparable performance of the proposed scheme with security enhancement.

To enhance reliability in location-based service (LBS) using a third party (TTP), in [78], a trustworthy middleware in the fog was presented to save significant partial data with dummy anonymity technology to support physical control, which can be assumed as actually trust. Thus, mobile users' partial significant information can be saved on a fog server to make sure manage well. The rules of similarity, intersection, practicability and correlation into consideration and the design of a dummy rotation (DR) algorithm with different characteristics were considered.

In [79], a bi-directional fuzzy logic-based trust management system (TMS) offered safe offloading, and corporation between fog nodes. This system permits a service requester (SR) to check the level of trust for a service provider (SP) and an SP to assay whether they can rely truthfully on the SR before establishing a communication. Direct trust computation is performed utilizing quality of service (QoS), quality of security (QoSec), degree of safety and social communications measures. The security evaluation shows that the proposed system is resilient against trust-related attacks. Also, the performance evaluation has illustrated that the TMS accomplishes a permissible degree of validity, reliability, and proficiency.

Table 4, explains some studies conducted security in fog computing using reliability are shown briefly.

5.2. Authentication and access control

The access level in fog includes four approaches:

1. **Access control by making behavioral identifier for the nodes**: each node through a specific identifier has the right to use and access the resources. This identifier may be built in a group or for a particular node.
2. **Access control using feature encryption and resources**: making specialized cryptography method for resources and access level control through the essential management process.
3. **Access control through certificate authority**: making identifiers that a process can use to complete a cryptography method to access resources and authorities.
4. **Pre-determined policy-based access control**: making a policy like a locality for a node in a region or having a level of energy for determining the authorities in a fog network.

In [64], a method was stated that the activation process of a node must be determined. A user profile is used to determine user behavior which registers all the behaviors of a node based on comparison with a regular user, issues an access certificate to different parts.

A technique was used in [80] for encryption and accessing different access levels. In this study and similar ones [81], generation, distribution, life cycle and key removal are set to optimize the access levels.

A certificate-based approach was proposed in [82] for cloud end, fog network, and IoT devices called Certificate Authority (CA). This approach is optimized by Dsouza et al. In [83], a method is presented to optimize security collaboration to make an access certificate to the resources.

In [84], an effective EASBF authentication scheme was demonstrated to secure fog-based IoV applications according to vehicle's identities. The scheme includes five parts: setup identity, enlistment, authentication, interchanging keys, agreement and certificate update. With the help of the elliptic curve cryptography, hash function, and Blockchain approach, the scheme achieves security characteristics such as confidentiality, integrity, authenticity, privacy, non-denial, and precise forward mystery. The security analysis shows that the scheme can resist effectively different

Table 4
Analyzing studies conducted reliability in fog computing.

References	Main idea	Mobility	Strengths	Weaknesses
Elmisery et al., 2016 [70]	Middleware security& presenting models for it	No	• Short time • High efficiency	• Failure to check all environment variables
Do Kim, 2009 [71]	Presenting models middleware security	No	• High efficiency	• Not defining test environment • High complexity
Soleymani et al., 2017 [72]	Creating a reliable middleware for Vehicle to convince the integrity and reliability of the program	Yes	• short time • High efficiency • Low cost • Proper scalability	• low cost • Proper scalability
Wang, et al., 2017 [73]	Creating a shared distribution system to prevent fraud	No	• High efficiency	• High cost • High time overhead
E. Onica, et al., 2016 [74]	Developing a PSS (Preserving Publish/Subscribe) system to prevent collusion	No	• High scalability • High availability	• High cost • High time overload
Dang and Hoang, 2017 [75]	Providing a region-based trust system	Yes	• Short time • High efficiency	• Not defining test environment
Y. Yao, et al., 2018 [76]	VF construction strategy and a VFS access strategy to achieve VFS trustworthy, reliability and security with preserved performance	Yes	• Short time • High efficiency	• Failure to check all environment variables
Koo et al., 2016 [77]	Creating a reliable middleware to improve safe storage	NO	• Short time • High efficiency	• High complexity
Wang et al., 2017 [78]	Selecting a third party to build a reliable middleware in fog to save partial major data with dummy anonymity technology to make certain trustworthy	NO	• High efficiency • Create a reasonable overhead	• Low scalability
Ogundoyin et al., 2021 [79]	Preparing a bi-directional fuzzy logic-based trust management system (TMS) for safe offloading and fog-to-fog corporation	NO	• High efficiency • short time	• High cost • Low availability • Failure to check all environment variables

attacks. Comparing the proposed model with the other available schemes shows the of the scheme's efficiency in the field of computation, transmission, and memory overheads.

According to the nature of fog computing, data is always seeking and unstable in fog, so that it should be modified all the time. For the purpose of preventing the forgery attack in fog computing, especially in VANETs, a lattice-based incremental signature scheme was offered in [85] that support an effective gradational authentication approach for the modified data in a fog environment without accessing the fogs to the original message and signature, so that the device does not need to save the message and its signature in the local memory. The scheme performs multi blocks and combined incremental operations. With the help of parallel computing or pre-computing, the proposed scheme's computational overhead decreases while the length of keys and signatures are qualified. The analysis result indicates the scheme can resist known attacks, and the limited resources of the fog nodes can be effectively saved.

Table 5 briefly shows some studies conducted about access level and their activity domain in fog.

5.2.1. Using ABE cryptography in fog

In [81], a method was proposed for making access level according to feature encryption called ABE. In this article, a method is suggested which is based on outsourcing and multi-tasker stability.

In [90], fog security concerns were stated. Due to analyzing data sharing problems, unauthorized people's information access was considered one of the most significant problems in the fog. In this paper, was mentioned that using the ABE encryption method separately, is not adequate for making appropriate access levels and solving access level problem and suggested, ciphertext-policy based approach and cryptography, a technique proposed for increasing security in fog and cloud connection.

In [91], a framework was developed for merging cloud, fog and IoT to manage saved data of industries and people. The model provided the background for the inevitable removal of data so that the confirmable data are removed and provided flexible access control on sensitive data. In the protocol, which is based on the ABE cryptography method, merely data owners and fog devices will collaborate in removing cloud information and confirming data removal; this feature causes the protocol to be implementable because of little delay time and real-time interaction with fog. Theoretical analysis shows that the function and operational requirements are reasonable. The results of implementing the protocol show that this protocol is feasible.

In [92], an outsourcing method with ABE cryptography was mentioned that is not a completely secure method against attacks and unauthorized access to data. An outsourcing practice is suggested with ABE cryptography considering some policies called CCA-secure and presented some experimental tests to prove the practicality of their method.

In [93], a novel fog computing e-learning structure was proposed. The solution expands the learning context from the cloud to the edge of the network. It can prosper the performance of learning data assessments, decreases the encrypting constraint in the field of computing overhead on user's devices by offloading section of encrypting overhead to fog nodes and prepares each item of data specified policy for access to learning context by encrypting the course and the exam with various cryptographic approaches like IBBE and CP-ABE. Security analysis displays that the structure can accomplish data confidentiality, fine-grained access control, collusion resistance and enforceability. The assessments illustrate that the solution is efficient, specifically in the field of encryption computation costs.

An outsourcing computing structure in vehicular fog computing (SE-VFC) was demonstrated in [94], which assigns some

Table 5
Analyzing the studies conducted about access control in fog.

References	Main idea	Mobility	Strengths	Weaknesses
Mandlekar et al., 2014 [64]	Access control by creating a behavioral identifier and recording each activity for the nodes	No	• Reasonable time overload • Low cost	• Failure to check key management system
Kim et al., 2014 [80]	Feature Cryptography	No	• High scalability • Low Complexity	• Not defining test environment • High time overhead
Fan et al., 2017 [81]	Designing of a feature-specific encryption system for fog environments	Yes	• High efficiency	• High time overhead • High cost
Alrawais et al., 2017 [82]	Creating an ABE-based approach for encryption-based access control	No	• High efficiency	• High complexity • High time overhead
Dsouza et al., 2014 [83]	Improving ABE	No	• High efficiency • Short time	• High complexity
Wu et al., 2021 [84]	Purposing an efficient authentication scheme over blockchain (EASBF) to secure fog-based IoV applications	Yes	• High efficiency • High availability • low complexity • low cost	• No checking all environmental variables
Wang et al., 2021 [85]	Implementing a lightweight, effective and secure authentication key exchange (AKE) scheme	Yes	• High efficiency • Short time • High scalability • low cost	• No checking all environmental variables
Jiang et al., 2018 [86]	Creating a certificate-based method for access levels	No	• High efficiency • High scalability	• High time overhead • High cost
Alrawais et al., 2017 [87]	Creating an CP-ABE method based on production policies and key management	Yes	• High efficiency • High scalability • Short time	• High complexity • High cost
Zhang et al., 2018 [88]	Creating and manage private keys in general management	No	• High scalability • High efficiency • Short time	• High complexity • High cost • Not defining test environment
Abdul et al., 2017 [89]	Creating a biometric method for encryption and decryption on edge devices and fog	No	• High efficiency • Targeted key management	• High complexity • High cost • High time overhead
Vohra, et al., 2018 [90]	Suggesting a ciphertext-policy based method and cryptography to increase security in fog and cloud connection	No	• High efficiency • Low cost	• Not defining test environment
Yu, et al., 2018 [91]	Developing a framework to merge cloud, fog and IoT to manage saved data of industries and people	Yes	• High efficiency • low complexity • low cost	• No checking all environmental variables
Zuo, et al., 2018 [92]	Suggesting an outsourcing method with ABE cryptography considering some CCA-secure policies practicality of their method.	Yes	• Short time • low cost	• High complexity • No checking all environmental variables
Amor, et al., 2020 [93]	Developing a novel fog assisted e-learning structure equipped with a fine-grained access control to learning subjects using IBBE and CP-ABE cryptographic techniques	No	• High efficiency • low complexity • Short time	• High cost due to the size of data
Liu et al., 2021 [94]	Preparing an outsourcing calculating structure in vehicular fog computing (SE-VFC)	Yes	• High efficiency • Short time • low cost	• Not defining test environment

encryption calculating to fog vehicles with calculating abilities. It also merges lightweight Boneh–Lynn–Shacham (BLS) signature and batch signature to obtain batch anonymous authentication in fog vehicles and ensure that the original vehicle can safely and effectively use real-time services with fine great of privacy. The proposed structure assays the integrity of outsourcing calculation outcomes prohibits unreliable fog vehicles from forging identities, steal and tamper with data. The assessment displays that the scheme can verify the fog vehicles by assigning calculation task and preserve their privacy, as well as tracking the harmful nodes with the CP-ABE method to ensure if the fog vehicles have truthfully fulfilled the posted calculating jobs.

5.3. Attacks

Since fog located at the cloud edges, it mostly does not have intense security levels; therefore, it is subject to many attacks. The attacks can be from a hostile internal node or using Man-In-The-Middle (MITM) attack model; fog will be exposed to information disclosure, damage or resource change, and so on [16].

In [16], different attacks were analyzed in a fog system using the division of workload on several fog nodes, and the results of attacks are measured using a destructive node on those nodes. While the results did not cause a solution to identify attacks, it showed the profound vulnerability of a fog network.

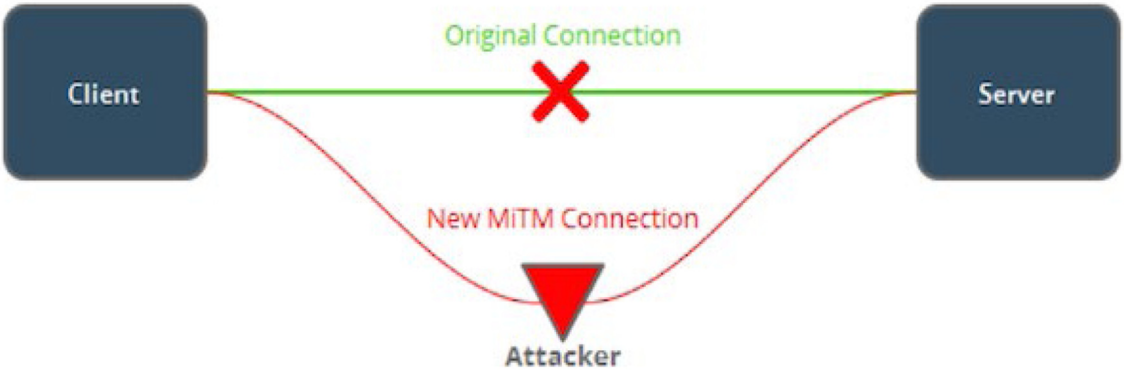

Fig. 10. Structure of a MITM attack in a fog [70].

A solution in [95] was presented to point out that the nodes at the edge of a network usually contain essential security information and roles; however, primarily due to the fog connection structure, it is highly vulnerable against internal destructive nodes. The proposed solution uses the Markov chain and Honey Pot technique to recognize intrusion in fog networks [95].

Most connections among network edge devices and the cloud are through a secure connection channel. If a person out of the network accesses the channel, s/he can bug or change the information. It is called MITM in the fog, which is shown in Fig. 10 [70].

This attack includes four stages [96]:

- Being located beside the vulnerable smart devices by an attacker.
- Using a fake fog certificate and sending it for the vulnerable device with content showing that the certificate is needed for subsequent device use.
- After receiving the certificate and its acceptance by the vulnerable device, the connection will be broken, and the attacker will be located between resource and device as an interface.

Performing the attack using a bug in the open flow-based channel that is the interface between the device and fog body is an important issue. In [97], to identify distributed anomaly detection of data integrity attacks in smart grid systems, addressing security- and data privacy-related concerns, a fog computing-based framework was deployed. The proposed protocol takes advantage of a distributed maximum likelihood (ML) estimator to illustrate the livability and efficacy of the framework and the distributed attack detection technique by carrying out a series of simulation experiments. The obtained results indicate preliminary to deploy fog computing technology in smart grid systems and chiefly to enhance cyber-security of power networks.

In [98], an anomaly-based IDS in a fog environment was implemented that transfers the available cloud-based security architecture to fog nodes. Since fog nodes perform offloading computation, the suggested structure uses the architecture for finding unusual traffic in the IoT network. The offered structure utilizes, a label-one-hot-encoding method for preliminary processing the arrival network traffic to convince that the measure of data stays the same and does not become tender. Also, it uses the correlation coefficient method for feature selection to decrease the size of data and build a light IDS. Analyzing the offered structure under various machine learning algorithms shows that the structure has a high detection precision and low false alert rate in detecting different IoT attacks.

The studies related to attacks are shown according to their activity domain in Table 6.

5.4. Privacy

Privacy is one of the users' significant concerns about their information in the fog because of different reasons.

The most important aspect of privacy, which were emphasized with the researches, is the node location being hidden. In [102], a method is introduced about hiding the location of vehicles (on the Internet of Vehicles (IOV) to support fog) from other nodes.

In addition to the location, other characteristics were also studied. In [70], the disclosure boundary between privacy and advertising and the identity boundary between oneself and others was surveyed and analyzed. In [103], a privacy method was demonstrated, which is appropriate for a homogeneous environment, and does not support heterogeneous fogs.

In [104], a dual key protocol for privacy was suggested that has the cryptography capability based on a bilateral agreement in identity protection.

In [105], a novel communication privacy-preserving range query structure in fog-enhanced IoT was proposed. With this scheme, the privacy of both the query range and the individual IoT device's data can be kept by utilizing BGN homomorphic encryption method. Moreover, the structure uses a range query expression, decomposition, and composition method to distinguish the range query that can accomplish $O(\sqrt{n})$ communication effectiveness. Comprehensive security analysis appears that the structure is indeed a privacy-preserving range query structure. The evaluation's results show that the suggested scheme is effective in low range query building cost and low correlation overhead.

In [106], the probability of making a one-time pad (OTP)-assisted encryption protocol with no packet loss was investigated; lesser time and energy costs compared to other protocols observed. The protocol will be tried out on wireless sensors, which are resource-restricted, and the result watched. The OTPs will be produced employing a random number generator inside the nodes.

Data gathering at a single fog collector node causes computational limitations on the node, which leads to high latency, abused reliability, and privacy problems. It shows the node to be a point of failure dignities. In [107], a data-gathering framework in fog, according to a Divide-and-Conquer technique, was demonstrated that separates and collects data due to the Level of Privacy (LoP) specified by data owners to rectify data privacy, data computing, and storage abilities in fog computing. The framework dispatches data among participating fog nodes due to the LoP approach to reduce the bottleneck of data at a single fog node and perform parallel processing and improve performance overhead. The analysis of privacy denotes the framework improves data privacy in

Table 6
Analyzing previous studies regarding attacks in fog.

References	Main idea	Mobility	Strengths	Weaknesses
Lee et al., 2015 [16]	Fog security testing against malicious attack nodes	No	• High efficiency • High scalability • Short time	• No checking environmental variables
Sohal et al., 2018 [95]	Testing attacks on network edge nodes and its security implications	Yes	• High efficiency	• No checking environmental variables • High time overhead • High complexity
Li et al., 2017 [96]	Checking MITM attacks in fog	No	• High efficiency	• No checking environmental variables • High time overhead • High complexity
Davoodi et al., 2020 [97]	Developing a fog-based framework to recognize distributed anomaly of data integrity attacks in smart grid applications	No	• High efficiency • Short time	• High complexity
Kumar et al., 2021 [98]	Designing an anomaly-based IDS using decentralizing cloud-based security architecture	No	• High efficiency • Low cost • High scalability	• No checking environmental variables • High complexity
Li et al., 2017 [99]	Identifying vulnerable nodes at the edge of the network	Yes	• High efficiency • Short time	• No checking environmental variables • High complexity
Koo et al., 2016 [100]	Detecting MITM attack based on CPU and memory properties and values	No	• High efficiency • Low energy • High scalability	• High complexity
Hu et al., 2017 [101]	Avoiding MITM attack using asymmetric encryption	No	• High efficiency • High scalability	

fog computing and can efficaciously resist internal and external attacks. It also decreases computational and memory overhead.

In Table 7, the analyzing of studies and their emphasis on privacy are shown.

5.5. Secure connection

There are two kinds of secure connection among the nodes of a fog network; the connection between fog nodes and IoT devices, and connection among the fog nodes. There may be some fake messages when communicating, and the attackers send incorrect information to the network.

The study in [115] was demonstrated that when data was transferred from the edge towards the cloud, the security in the fog scope must be prepared to facilitate accessing the resources, and the scope of resources must be solid and adjustable. In this study, a stable and integrated security mechanism was designed for Fog–Cloud connections alternately and flexibly. This design had the advantage of confronting the network invalid connections and uncontrolled change of messages in diverse security conditions of fog network and based on the different needs of applications.

In [116], a method was also suggested to optimize secure connection in fog by designing a routing protocol to increase security and also optimizing information transferred based on the unknown resources.

In [117], a blockchain-based lightweight anonymous authentication (BLA) technology for distributed VFS was proposed, which is planned for driving vehicles. BLA can accomplish some subsequent profits. (1) Figuring out a fluid cross-data center authentication so that a vehicle can choose if to be re-authenticated or not when it gets in a new fog datacenter. (2) Attaining anonymity and privileging vehicle users the obligation of maintaining their privacy. (3) It is lightweight by accomplishing no interactivity between vehicles and service managers (SMs) and omitting the communication among SMs in the authentication operation, which considerably decreases the correlation latency. (4) Persisting the attack that the database controlled by one center is interfered with. BLA accomplishes these benefits by efficiently integrating novel cryptographic and blockchain method. These safety highlights are illustrated by performing security analysis. The spacious simulations demonstrate the excellent performance and feasibility of BLA.

The anonymous and secure aggregation scheme (ASAS) in fog-based computing was proposed in [118]. In the ASAS model, a fog node collects data from end nodes and directs the collected data to the cloud server. ASAS scheme aids the fog nodes to upload their data to PCS. It leads the scheme to save bandwidth between the fog node and PCS as well as, preserving the identities of end devices by using pseudonyms and assurances of data secrecy through a homomorphic encryption method.

A hierarchical key pre-distribution structure according to the transversal design and residual theorem (TD-R) was presented in [119] for great mobile fog networks with multi-clouds. The structure aims to disclose that TD-R is the key pre-distribution structure for building up secure intra and inter-fog nodes' communication and intra and inter-end nodes with medium processes of connecting various parts of the network. The out comings point that the presented structure improves network scalability, so long as it reduces memory usage and node storage overhead.

Analyzing the studies in fog shows the importance of secure connection from the viewpoint of researchers about security in fog. In Table 8, the aims of these studies are presented.

Table 7
The studies conducted about privacy.

References	Main idea	Mobility	Strengths	Weaknesses
Elmisery et al., 2016 [70]	Determining the boundary of privacy disclosure	No	• Short time • High efficiency •	• No checking environmental variables
Wang et al., 2017 [78]	Using a preserved nickname with privacy	Yes	• High efficiency • Create a reasonable overhead	• Low Scalability
Lu, Rongxing, 2018 [95]	Privacy preserved	No	• Low cost • Low time overhead	• No checking environmental variables
Boakye-Boateng, Kwasi, et al., 2019 [96]	Resource constraint	Yes	• Low cost • Reduce energy	• Low Scalability
Dong et al., 2015, Yang et al., 2018 [108,109]	Location cryptography	Yes	• Accessibility • Scalability • Short time	• High complexity • High cost
Kang et al., 2017, Yang et al., 2017 [102,110]	Providing an outline for protecting privacy by using hiding	Yes	• Accessibility • Scalability	• High complexity
Wang et al., 2017, Du et al., 2017 [73,111]	Separator queries based on privacy	No	• High efficiency	• High cost • High time overhead
Lu et al., 2017 [103]	Hiding data privacy by using the aggregated data	No	• Short time • Low cost • High availability	• No checking environmental variables
Zuo et al., 2018, Al Hamid et al., 2017 [104,112]	Encrypting and decrypt information	No	• High efficiency • Short time • High availability	• High complexity • No checking environmental variables • Failure to consider key management
Hu et al., 2017, Basudn et al., 2017, Wang et al., 2017 [68,113,114]	Designing a secure protocol for privacy	No	• Short time • Low complexity	• No checking environmental variables
Sarwar et al., 2021 [107]	Providing a lightweight privacy preserving data collecting framework	No	• High efficiency • High availability • Short time	• No checking environmental variables • High complexity • High cost

Table 8
The studies conducted about secure connection in fog.

References	Main idea	Mobility	Strengths	Weaknesses
B. Mukherjee, et al., 2017 [115]	Preparing a secure and seamless security mechanism for Fog–Cloud communications	No	• Short time • High efficiency	• No checking environmental variables
W. Fang, et al., 2017 [116]	Designing a routing protocol to enhance security and improve the transfer of information based on the anonymity of resources	Yes	• High efficiency • Short time	• No checking environmental variables
Yao, Yingying, et al, 2019 [117]	lightweight anonymous authentication (BLA) mechanism	Yes	• Flexible increase • High efficiency • Scalability	• High cost • Delay increase
Wang et al., 2017 [118]	Providing a homogeneous encryption method when loading data from edge devices to the cloud in order to guarantee the security of information exchange channel	Yes	• High efficiency • High availability	• High cost • High time overhead
Masael, et al., 2020 [119]	Designing a hierarchical key pre-distribution structure using TD-R for great mobile fog networks with multi-clouds	Yes	• Scalability • Short time • Low cost	• No checking environmental variables

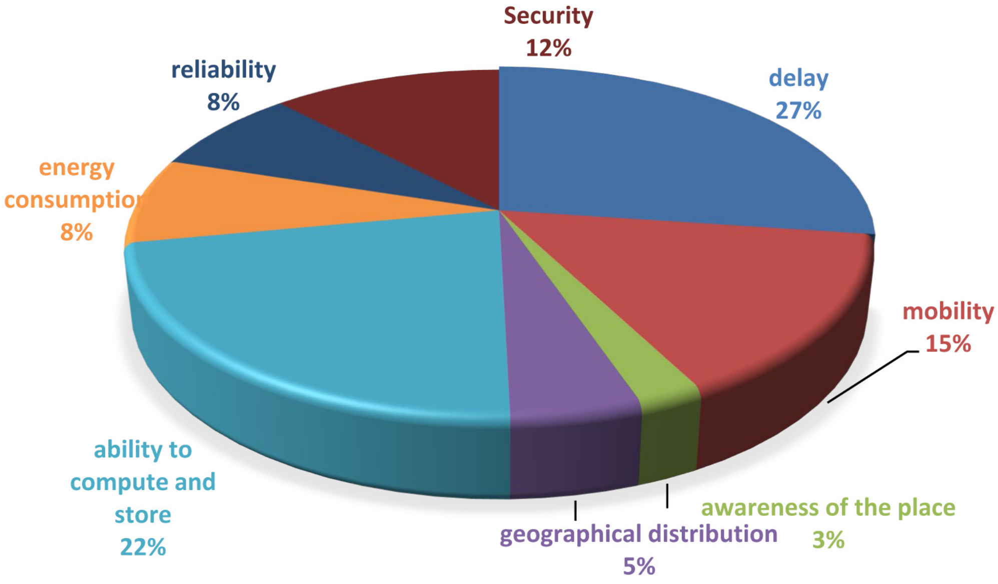

Fig. 11. Percentage of the differences between fog and cloud computing.

5.6. Service accessibility, security applications and secure sharing technology

Attacks like DOS lead to losing the services in fog. While this special case can be categorized as part of attacks, making unnecessary resources inaccessible is a method to reduce the effects of these attacks in fog [120].

In [25], some other challenges was also presented about fog and its uses which are: web optimization, virtual radio access, smart measurement, G5 mobile phone networks, surveillance video processing, healthcare systems, transport and road safety networks, food traceability, spoken data, brain and computer interface, resource management, energy reduction, catastrophe response and military and security environment.

6. Discussion

This section tries to answer the questions in Section 3. These answers will be written in the articles as mentioned. Also, they are described statistically in this section.

- Q1: What are the differences between the scope of fog computing and cloud computing, and how fog computing can help to improve the current challenges in cloud computing?

Differences between fog and cloud computing are discussed in terms of some issues like delay, real-time support, mobility, awareness of the place, number of serving nodes, geographical distribution, distance to service recipients, service location, the necessary environment for activity, communication model, dependence on the quality of the central network, bandwidth consumption, ability to compute and store, energy consumption. According to Fig. 11, we considered that delay has the highest percentage of differences between fog and cloud computing by 27% in these studies. Also, ability to compute and store has 22%, mobility has 15%, security has 12%, and reliability and energy consumption have 8%, geographical distribution has 5%, and awareness of the place has 3% of issues in discrepancy within the fog and cloud computing.

- Q2: What are the security-related challenges in fog computing?

Security is one of the key challenges in fog computing. The security challenges of fog computing can be perceived in Fig. 6, including Reliability, Authentication and Access control, Attacks, Privacy, Secure connection, Other cases like Service accessibility, Security applications and Secure sharing technology. Fig. 12 shows the statistical percentage of fog computing's security challenges according to existing researches. We observed privacy by 22% has the highest rate of fog security challenges in the researches. In addition, 20% of studies demonstrates authentication-access control, 19% express reliability and attacks as security challenges. Moreover, we perceived that 12% of the recent papers remark service accessibility, security applications and secure sharing technology as some fog security challenges. Finally, we realized that 8% of the existing papers present secure connection as a fog security challenge.

- Q3: What are the current solutions to fog computing security challenges and their strengths and weaknesses?

There are many solutions and methods to solve or improve security challenges in fog computing, but those have some strengths and weaknesses presented in Figs. 13 and 14. Some variables that can be used to compare these methods are included: Confidentiality, Accessibility and Integrity. To provide reliable services and preserved data privacy, various security protocols must be prepared in fog nodes, including authenticated key authentication, data encryption, digital signature and spam detection. If the protocols used are insufficient, many computing resources will be wasted, and response time will be increased. We observed 39% of researches present high efficiency, 25% short time, 13% low cost, 12% high scalability, 6% high availability and 5% low complexity as the strengths in the current solutions for security challenges in fog computing. Also, the statistical rate of the analysis recommends that high complexity has the most rate in evaluating of the weaknesses in the solution for security challenges in fog by 27%. We observed that 24% of the case studies present no checking environmental variables, 19% high cost overhead and 14% high time as weaknesses. In addition, not defining test environment has 6%, low scalability has 4%, failure to check all environment variables and low availability have 3% of portions in the studies.

- Q4: What general vision is imaginable about the future of security in fog computing, and what new solutions can be proposed?

According to previous studies and the results for those interested in security in fog, the following approaches can be proposed as the open issues that are not addressed indeed by the research papers:

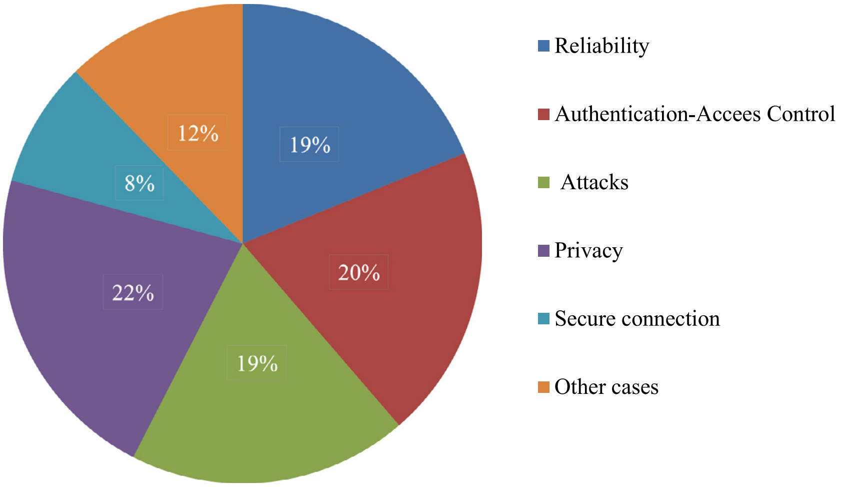

Fig. 12. Percentage of the fog computing's current security challenges.

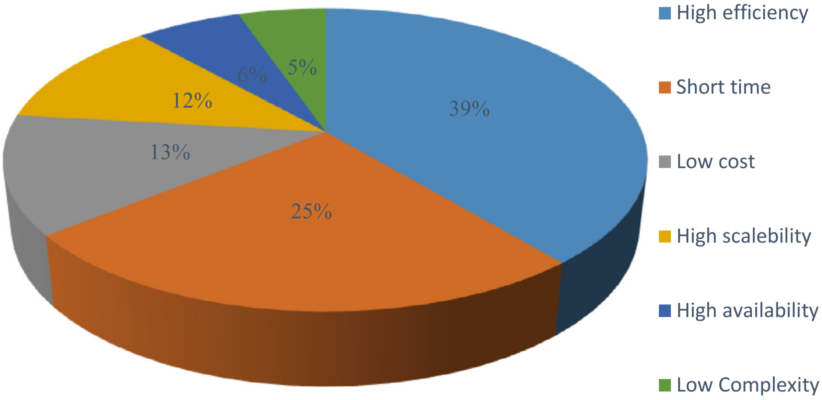

Fig. 13. Percentage of the strengths in current solution for security challenges in fog computing.

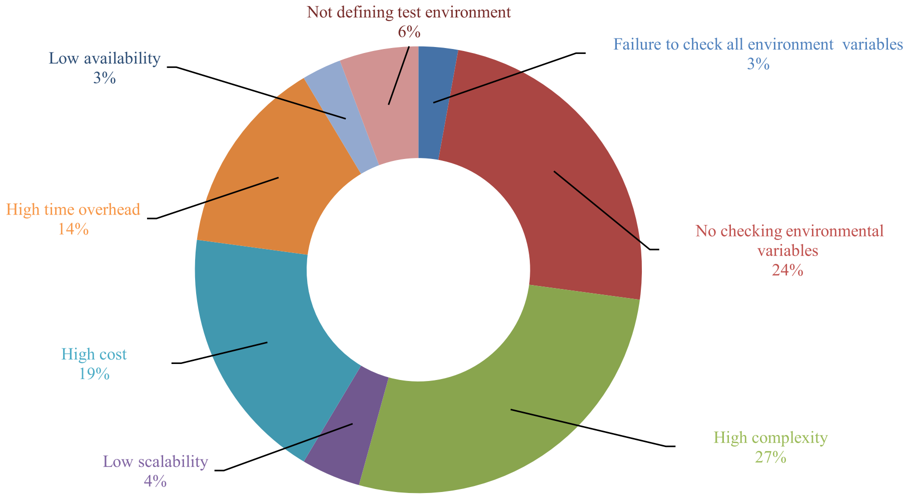

Fig. 14. Percentage of the weaknesses in current solution for security challenges in fog computing.

- Analyzing the models of reliability increase in fog
- Optimizing fog function considering security points by reducing computing overhead and reducing resource consumption
- Developing reliable models using exchanged data structures
- Using other methods of encryption and decryption and measuring its computing load on fog function
- Managing and organizing region-based reliability and developing procedures to identify network representatives and brokers
- A combination of using certificate development or encryption method to develop regions and access level
- Developing new methods computing security and reliability level and so on.

- Developing new methods for intrusion detection in fog based on anomaly detection
- Using behavior similarity measurement methods in fog
- Developing methods estimating the fog network's requirements, including the necessity of applying real-time, mobility and so on.

7. Future directions and open issues

Although there have been many studies in this field, due to the fog security significance as well as achieving the technical taxonomy in Section 4 and the results obtained in Section 6, there are still many open issues which we analyzed in some categories.

- *Trustworthy environment:* a trustworthy environment for fog is a primary concern for data computing, data access and data storage on fog networks. Trustworthy environments for the fog prepare a secure interconnection between IoT devices and the cloud to support network services. The key challenge of this issue is that fog nodes prepare acquisitive use of numerous diverse services, even composited services to the users that should be safe. Given that the dimensions of a safe environment for the fog have not been explicitly defined [66,67] and the specific monitoring and supervising in the fog has not been specified [66], identifying the characteristics of a safe environment and establishing a protected environment through it is a matter.
- *Security and reliability analyzing:* the concept of reliability with the approach of fog nodes can perform secure operations without problems and deliver results to stakeholders, is a crucial concern. Reliability has not been carried out in previous researches correctly [68–71]. There is also no coordination between security approaches, and activities of a fog network [67–71,73]. In addition, most of the security features reduce the quality and performance of a fog network. Moreover, designed security solutions cannot guarantee standard service agreements like SLA, and they are such a barrier to them [64,74,75,77,121]. The main challenge of this topic is maintaining coordination between the quality of fog services and security issues. This challenge conducts to pay attention to preparing new environments and protocols for security fractures, especially with the focus on reliability.
- *Access level to resources analyzing:* a fundamental challenge with existing methods is the lack of security criteria at the access level. Another issue that could be considered is the quality of the access right that has not been applied in any of reviewed cases [9,16–18,23–25,29–34,36–38,40–42,59,64–68,70–75,77,78,80–92,95,96,98–104,107–116,118,120–127]. Therefore, it is necessary to define a criterion for measuring the level of security in fog networks.
- *Collusion prevention:* broker is the most essential part of a PSS system. The requests are sent for brokers and a connection between two pieces of a fog system or between fog and cloud system prepared by a broker. Preserving broker nodes security is a considerable matter when requests were delivered to a cloud data center or between other nodes. In the previous researches, there are no solutions if a node broker was an attacker, and there are no methods to confront it in collusion prevention part. Concerning the importance of this topic, it seems necessary to develop strategies to predict hostile nodes for server-side attacks and deal with this type of security risk [70–75].
- *Backing up and restoring data:* using a backup scenario of data retention is a crucial challenge, according to the importance and necessity of data on a fog network. Unexpected hardware and software problems can cause fog networks to lose important information. If the data in fog is removed, the fog network cannot continue to live and serve, or if the data related to nodes' identity is damaged, it will impose a considerable network risk. There is a need to back up and restore the fog data, as no previous papers have been made on this topic [91,93,107].
- *Behavior of fog nodes:* analyzing the activity of fog nodes and detecting if the fog node abuses activity is conducted to detect intrusion. Recent researches have not focused on behavior-based intrusion detection systems. Since focusing on behavior is one of the hallmarks of intrusion detection, it is a key challenge. Developing new methods for intrusion detection in fog networks based on anomaly detection and user behavior similarity measurement methods are essential [70,94,96].
- *Overhead of cryptography mechanisms:* due to the nature of fog nodes and their limited resources for computing and storing data, applying appropriate cryptography methods on fog networks is a key challenge according to the impact of resource consumption overhead related to the employed cryptography methods. There are no precise mechanisms proposed about cryptography mechanisms to calculate the network overhead of these systems [96,98–100,107]. Applying a mechanism for measuring the computing load of cryptography methods can be effective for choosing the appropriate network approach and improving the quality of services and security factors in the fog.
- *Mobility:* According to the nation of fog nodes that have mobility, some features in the fog, such as security, are affected and considered by different methods and approaches compare to fixed nodes. Estimating necessary conditions for establishing a fog network is a significant challenge. A mechanism for evaluating conditions needed for a fog network, including the requirements related to applying mobility, would be essential [71,73,74,77–80,82,83,86,88–90,93,96–98,101,104,105,107,111,113,119].

8. Conclusion

Fog computing is a kind of distributed computing that decreases computation on the cloud by providing an intermediate layer between the Internet of Things (IoTs) devices and the cloud. Fog computing aids the services to be more efficiently and effectively, but it acts weakly against security threats. Also, analyzing the quality of security services and their threat identification methods seems to be a barrier to the benefits of fog. Coordinating security solutions with different devices in different scenarios may challenge the security plans to be implemented for the fog environment. Despite all these issues, we can point out that the advantages of fog can be very effective according to information and technology society needs. However, benefiting from these advantages requires designing new solutions which can model and cover security issue in fog with six challenges as mentioned earlier.

In this paper, we analyzed recent implements of fog computing. Challenges in fog computing are discussed here concerning structural, service and security-relevant aspects. Considering the specified and crucial security issues and concerns in the fog environment, a helpful taxonomy has also been presented. Our taxonomy classifies and analyzes the available studies due to their approaches for addressing the security challenges. We employed an SLR method by using the exploration queries on 232 researches published between 2014 and 2021. Finally, we analyzed 79 papers that concentrated on security challenges in fog computing to respond the provided technical questions. We found out that delay by 27% has the highest percentage of issues in differences between fog and cloud computing. Also, ability to compute, and store has 22%, mobility has 15%, security has 12% and reliability and energy consumption have 8%, geographical distribution has 5% and awareness of the place has 3% of quotas according to Q1. Concerning Q2 and analyzing the security challenges in fog computing, we observed privacy is the most percentage which is discussed in 22% of researches, authentication-access control in 20%, reliability and attacks in 19%, service accessibility, security applications and secure sharing technology in 12% and secure connection in 8% of researches. According to Q3, high efficiency by 39% is the most frequent factor related to strengths in the current solutions for security challenges in fog, short time has 25%, low cast has 13%, high scalability has 12%, high availability has 6%, and low complexity has 5% of portions in the literature. Concerning Q4 and comparing assessment factors, high complexity by 27% has the most percentage in evaluating weaknesses in the current solution for security challenges in fog. Also, no checking environmental variables has 24%, high cost has 19%, high time overhead has 14%, not defining test environment has 6%, low scalability has 4%, and failure to check all environment variables has 3% of the studies. As well as, according to the investigation, we proposed some promising research trends to access further security points that can be pursued in the future, such as using new methods for estimation, detection and development of security issues in fog networks. Besides, more precise coordination between security activities and quality of services, reliability, computing overhead and resource consumption will be necessary for fog networks.

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

[1] C. Avasalcai, I. Murturi, S. Dustdar, Edge and fog: A survey, use cases, and future challenges, in: Fog Computing: Theory and Practice, 2020, pp. 43–65.

[2] M.R. Raza, A. Varol, N. Varol, Cloud and fog computing: A survey to the concept and challenges, in: 2020 8th International Symposium on Digital Forensics and Security (ISDFS), IEEE, 2020, pp. 1–6.

[3] C.-M. Chen, Y. Huang, K.-H. Wang, S. Kumari, M.-E. Wu, A secure authenticated and key exchange scheme for fog computing, Enterp. Inf. Syst. (2020) 1–16.

[4] M. Mukherjee, M.A. Ferrag, L. Maglaras, A. Derhab, M. Aazam, Security and privacy issues and solutions for fog, fog and fogonomics: Challenges and practices of fog computing, Commun. Netw. Strat. Econ. (2020) 353–374.

[5] P. Asghari, A.M. Rahmani, H.H.S. Javadi, Internet of things applications: A systematic review, Comput. Netw. 148 (2019) 241–261.

[6] F. Asadpour, S. Ghanbari, Presenting a new method of authentication for the internet of things based on RFID, in: International Conference on Soft Computing and Data Mining, Springer, 2018, pp. 506–516.

[7] P. Asghari, A.M. Rahmani, H.H.S. Javadi, Service composition approaches in IoT: A systematic review, J. Netw. Comput. Appl. 120 (2018) 61–77.

[8] J. Han, C.-S. Choi, W.-K. Park, I. Lee, S.-H. Kim, Smart home energy management system including renewable energy based on ZigBee and PLC, IEEE Trans. Consum. Electron. 60 (2) (2014) 198–202.

[9] S. Wang, X. Zhang, Y. Zhang, L. Wang, J. Yang, W. Wang, A survey on mobile edge networks: Convergence of computing, caching and communications, IEEE Access 5 (2017) 6757–6779.

[10] S. Tu, Muhammad Waqas, Sadaqat Ur Rehman, Talha Mir, Zahid Halim, Iftekhar Ahmad, Social phenomena and fog computing networks: A novel perspective for future networks, in: IEEE Transactions on Computational Social Systems (2021). Social Phenomena and Fog Computing Networks: A Novel Perspective for Future Networks, Ieee, 2021.

[11] L. Atziori, A. Iera, G. Morabito, The Internet of Things: A Survey COMPUTER NETWORKS, 2010.

[12] R. Deng, R. Lu, C. Lai, T.H. Luan, H. Liang, Optimal workload allocation in fog-cloud computing toward balanced delay and power consumption, IEEE Internet Things J. 3 (6) (2016) 1171–1181.

[13] M.M. Mahmoud, J.J. Rodrigues, K. Saleem, J. Al-Muhtadi, N. Kumar, V. Korotaev, Towards energy-aware fog-enabled cloud of things for healthcare, Comput. Electr. Eng. 67 (2018) 58–69.

[14] B.Z. Abbasi, M.A. Shah, Fog computing: Security issues, solutions and robust practices, in: 2017 23rd International Conference on Automation and Computing (ICAC), IEEE, 2017, pp. 1–6.

[15] X.-Q. Pham, E.-N. Huh, Towards task scheduling in a cloud-fog computing system, in: 2016 18th Asia-Pacific Network Operations and Management Symposium (APNOMS), IEEE, 2016, pp. 1–4.

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

[17] D. Evans, The internet of things: How the next evolution of the internet is changing everything, CISCO White Paper 1 (2011) (2011) 1–11.

[18] H. Ning, H. Liu, J. Ma, L.T. Yang, R. Huang, Cybermatics: Cyber–physical–social–thinking hyperspace based science and technology, Future Gener. Comput. Syst. 56 (2016) 504–522.

[19] K. Xue, J. Hong, Y. Ma, D.S. Wei, P. Hong, N. Yu, Fog-aided verifiable privacy preserving access control for latency-sensitive data sharing in vehicular cloud computing, IEEE Netw. 32 (3) (2018) 7–13.

[20] L. Ferretti, M. Marchetti, M. Colajanni, Fog-based secure communications for low-power IoT devices, ACM Trans. Internet Technol. (TOIT) 19 (2) (2019) 27.

[21] S. Soo, C. Chang, S.N. Srirama, Proactive service discovery in fog computing using mobile ad hoc social network in proximity, in: 2016 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2016, pp. 561–566.

[22] V. Moysiadis, P. Sarigiannidis, I. Moscholios, Towards distributed data management in fog computing, Wirel. Commun. Mob. Comput. 2018 (2018).

[23] M. Mukherjee, et al., Security and privacy in fog computing: Challenges, IEEE Access 5 (2017) 19293–19304.

[24] Y. Wang, T. Uehara, R. Sasaki, Fog computing: Issues and challenges in security and forensics, in: 2015 IEEE 39th Annual Computer Software and Applications Conference, vol. 3, IEEE, 2015, pp. 53–59.

[25] S. Khan, S. Parkinson, Y. Qin, Fog computing security: a review of current applications and security solutions, J. Cloud Comput. 6 (1) (2017) 19.

[26] G. Javadzadeh, A.M. Rahmani, Fog computing applications in smart cities: A systematic survey, Wirel. Netw. 26 (2) (2020) 1433–1457.

[27] W. Almobaideen, M. Altarawneh, Fog computing: survey on decoy information technology, Int. J. Secur. Netw. 15 (2) (2020) 111–121.

[28] K.H. Abdulkareem, et al., A review of fog computing and machine learning: Concepts, applications, challenges, and open issues, IEEE Access 7 (2019) 153123-153140.

[29] C.G.C. Index, Forecast and Methodology, 2014-2019 White Paper, White Paper, Cisco Systems, 2014.

[30] A.D. Josep, R. Katz, A. Konwinski, L. Gunho, D. Patterson, A. Rabkin, A view of cloud computing, Commun. ACM 53 (4) (2010).

[31] T. Qiu, K. Zheng, H. Song, M. Han, B. Kantarci, A local-optimization emergency scheduling scheme with self-recovery for a smart grid, IEEE Trans. Ind. Inf. 13 (6) (2017) 3195–3205.

[32] F. Bonomi, R. Milito, P. Natarajan, J. Zhu, Fog computing: A platform for internet of things and analytics, in: Big Data and Internet of Things: A Roadmap for Smart Environments, Springer, 2014, pp. 169–186.

[33] M. Hajibaba, S. Gorgin, A review on modern distributed computing paradigms: Cloud computing, jungle computing and fog computing, J. Comput. Inf. Technol. 22 (2) (2014) 69–84.

[34] S. Sarkar, S. Misra, Theoretical modelling of fog computing: a green computing paradigm to support IoT applications, Iet Netw. 5 (2) (2016) 23–29.

[35] P. Habibi, M. Farhoudi, S. Kazemian, S. Khorsandi, A. Leon-Garcia, Fog computing: A comprehensive architectural survey, IEEE Access 8 (2020) 69105–69133.

[36] P. Varshney, Y. Simmhan, Demystifying fog computing: Characterizing architectures, applications and abstractions, in: 2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC), IEEE, 2017, pp. 115–124.

[37] W. Shi, J. Cao, Q. Zhang, Y. Li, L. Xu, Edge computing: Vision and challenges, IEEE Internet Things J. 3 (5) (2016) 637–646.

[38] A.A. Alsaffar, H.P. Pham, C.-S. Hong, E.-N. Huh, M. Aazam, An architecture of iot service delegation and resource allocation based on collaboration between fog and cloud computing, Mob. Inf. Syst. 2016 (2016).

[39] M. Kazemi, S. Ghanbari, M. Kazemi, Divisible load framework and close form for scheduling in fog computing systems, in: International Conference on Soft Computing and Data Mining, Springer, 2020, pp. 323–333.

[40] R. Roman, J. Lopez, M. Mambo, Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges, Future Gener. Comput. Syst. 78 (2018) 680–698.

[41] E. Ahmed, M.H. Rehmani, Mobile Edge Computing: Opportunities, Solutions, and Challenges, Elsevier, 2017.

[42] A.V. Dastjerdi, R. Buyya, Fog computing: Helping the Internet of Things realize its potential, Computer 49 (8) (2016) 112–116.

[43] P. Zhang, J.K. Liu, F.R. Yu, M. Sookhak, M.H. Au, X. Luo, A survey on access control in fog computing, IEEE Commun. Mag. 56 (2) (2018) 144–149.

[44] K. Hong, D. Lillethun, U. Ramachandran, B. Ottenwälder, B. Koldehofe, Mobile fog: A programming model for large-scale applications on the internet of things, in: Proceedings of the Second ACM SIGCOMM Workshop on Mobile Cloud Computing, ACM, 2013, pp. 15–20.

[45] S. Cirani, G. Ferrari, N. Iotti, M. Picone, The iot hub: a fog node for seamless management of heterogeneous connected smart objects, in: 2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking-Workshops (SECON Workshops), IEEE, 2015, pp. 1–6.

[46] N.K. Giang, M. Blackstock, R. Lea, V.C. Leung, Developing iot applications in the fog: A distributed dataflow approach, in: 2015 5th International Conference on the Internet of Things (IOT), IEEE, 2015, pp. 155–162.

[47] V. Gazis, A. Leonardi, K. Mathioudakis, K. Sasloglou, P. Kikiras, R. Sudhaakar, Components of fog computing in an industrial internet of things context, in: 2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking-Workshops (SECON Workshops), IEEE, 2015, pp. 1–6.

[48] M.A. Al Faruque, K. Vatanparvar, Energy management-as-a-service over fog computing platform, IEEE Internet Things J. 3 (2) (2015) 161–169.

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

[50] L. Gu, D. Zeng, S. Guo, A. Barnawi, Y. Xiang, Cost efficient resource management in fog computing supported medical cyber–physical system, IEEE Trans. Emerg. Top. Comput. 5 (1) (2015) 108–119.

[51] D. Zeng, L. Gu, S. Guo, Z. Cheng, S. Yu, Joint optimization of task scheduling and image placement in fog computing supported software-defined embedded system, IEEE Trans. Comput. 65 (12) (2016) 3702–3712.

[52] T.N. Gia, et al., Low-cost fog-assisted health-care IoT system with energy-efficient sensor nodes, in: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE, 2017, pp. 1765–1770.

[53] M. Ahmad, M.B. Amin, S. Hussain, B.H. Kang, T. Cheong, S. Lee, Health fog: a novel framework for health and wellness applications, J. Supercomput. 72 (10) (2016) 3677–3695.

[54] E.Z. Abdevand, S. Ghanbari, Z. Umarova, Z. Iztayev, Introducing a New Intrusion Detection Method in The SDN Network to Increase Security Using Decision Tree and Neural Network.

[55] S. Chakraborty, S. Bhowmick, P. Talaga, D.P. Agrawal, Fog networks in healthcare application, in: 2016 IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), IEEE, 2016, pp. 386–387.

[56] A. Monteiro, H. Dubey, L. Mahler, Q. Yang, K. Mankodiya, Fit: A fog computing device for speech tele-treatments, in: 2016 IEEE International Conference on Smart Computing (SMARTCOMP), IEEE, 2016, pp. 1–3.

[57] B. Negash, et al., Leveraging fog computing for healthcare IoT, in: Fog Computing in the Internet of Things, Springer, 2018, pp. 145–169.

[58] A.M. Rahmani, et al., Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach, Future Gener. Comput. Syst. 78 (2018) 641–658.

[59] R. Mahmud, R. Kotagiri, R. Buyya, Fog computing: A taxonomy, survey and future directions, in: Internet of Everything, Springer, 2018, pp. 103–130.

[60] P. Zhang, M. Zhou, G. Fortino, Security and trust issues in Fog computing: A survey, Future Gener. Comput. Syst. 88 (2018) 16–27.

[61] J. Dizdarević, F. Carpio, A. Jukan, X. Masip-Bruin, A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration, ACM Comput. Surv. 51 (6) (2019) 116.

[62] A. Yousefpour, et al., All one needs to know about fog computing and related edge computing paradigms: A complete survey, J. Syst. Archit. (2019).

[63] J. Yakubu, H.A. Christopher, H. Chiroma, M. Abdullahi, Security challenges in fog-computing environment: a systematic appraisal of current developments, J. Reliab. Intell. Environ. (2019) 1–25.

[64] V.G. Mandlekar, V. Mahale, S.S. Sancheti, M.S. Rais, Survey on fog computing mitigating data theft attacks in cloud, Int. J. Innov. Res. Comput. Sci. Technol 2 (2014) 13–16.

[65] P. Kumar, N. Zaidi, T. Choudhury, Fog computing: Common security issues and proposed countermeasures, in: 2016 International Conference System Modeling & Advancement in Research Trends (SMART), IEEE, 2016, pp. 311–315.

[66] I. Stojmenovic, S. Wen, X. Huang, H. Luan, An overview of fog computing and its security issues, Concurr. Comput.: Pract. Exper. 28 (10) (2016) 2991–3005.

[67] I. Stojmenovic, S. Wen, The fog computing paradigm: Scenarios and security issues, in: 2014 Federated Conference on Computer Science and Information Systems, IEEE, 2014, pp. 1–8.

[68] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, X. Yao, Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things, IEEE Internet Things J. 4 (5) (2017) 1143–1155.

[69] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, R.M. Parizi, K.-K.R. Choo, Fog data analytics: A taxonomy and process model, J. Netw. Comput. Appl. 128 (2019) 90–104.

[70] A.M. Elmisery, S. Rho, D. Botvich, A fog based middleware for automated compliance with OECD privacy principles in internet of healthcare things, IEEE Access 4 (2016) 8418–8441.

[71] H. Do Kim, Applying consistency-based trust definition to collaborative filtering, KSII Trans. Internet Inf. Syst. 3 (4) (2009).

[72] S.A. Soleymani, et al., A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing, IEEE Access 5 (2017) 15619–15629.

[73] Q. Wang, D. Chen, N. Zhang, Z. Ding, Z. Qin, PCP: A privacy-preserving content-based publish–subscribe scheme with differential privacy in fog computing, IEEE Access 5 (2017) 17962–17974.

[74] E. Onica, P. Felber, H. Mercier, E. Rivière, Confidentiality-preserving publish/subscribe: A survey, ACM Comput. Surv. 49 (2) (2016) 27.

[75] T.D. Dang, D. Hoang, Protection model for fog computing, in: 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC), IEEE, 2017, pp. 32–38.

[76] Y. Yao, X. Chang, J. Mišić, V. Mišić, Reliable and secure vehicular fog service provision, IEEE Internet Things J. 6 (1) (2018) 734–743.

[77] D. Koo, Y. Shin, J. Yun, J. Hur, A hybrid deduplication for secure and efficient data outsourcing in fog computing, in: 2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), IEEE, 2016, pp. 285–293.

[78] T. Wang, et al., Trajectory privacy preservation based on a fog structure for cloud location services, IEEE Access 5 (2017) 7692–7701.

[79] S.O. Ogundoyin, Ismaila Adeniyi Kamil, A trust management system for fog computing services, Internet of Things 14 (2021) 100382, A trust management system for fog computing services, *Elsevier:Internet of Things* 2021.

[80] H.-W. Kim, J.-H. Kim, J.H. Park, Y.-S. Jeong, Time pattern locking scheme for secure multimedia contents in human-centric device, Sci. World J. 2014 (2014).

[81] K. Fan, J. Wang, X. Wang, H. Li, Y. Yang, A secure and verifiable outsourced access control scheme in fog-cloud computing, Sensors 17 (7) (2017) 1695.

[82] A. Alrawais, A. Alhothaily, C. Hu, X. Cheng, Fog computing for the internet of things: Security and privacy issues, IEEE Internet Comput. 21 (2) (2017) 34–42.

[83] C. Dsouza, G.-J. Ahn, M. Taguinod, Policy-driven security management for fog computing: Preliminary framework and a case study, in: Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI 2014), IEEE, 2014, pp. 16–23.

[84] T.-Y. Wu, Zhiyuan Lee, Lei Yang, Jia-Ning Luo, Raylin Tso, Provably secure authentication key exchange scheme using fog nodes in vehicular ad hoc networks, J. Supercomput. (2021) 1–29, EASBF: An efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles, Springers:The Journal of Supercomputing, 2021.

[85] F. Wang, Junquan. Wang, Wenfeng. Yang, Efficient incremental authentication for the updated data in fog computing, Future Gener. Comput. Syst. 114 (2021) 130–137, Efficient incremental authentication for the updated data in fog computing. Elsevier:Future Generation Computer Systems, 2021.

[86] Y. Jiang, W. Susilo, Y. Mu, F. Guo, Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing, Future Gener. Comput. Syst. 78 (2018) 720–729.

[87] A. Alrawais, A. Alhothaily, C. Hu, X. Xing, X. Cheng, An attribute-based encryption scheme to secure fog communications, IEEE Access 5 (2017) 9131–9138.

[88] P. Zhang, Z. Chen, J.K. Liu, K. Liang, H. Liu, An efficient access control scheme with outsourcing capability and attribute update for fog computing, Future Gener. Comput. Syst. 78 (2018) 753–762.

[89] W. Abdul, Z. Ali, S. Ghouzali, B. Alfawaz, G. Muhammad, M.S. Hossain, Biometric security through visual encryption for fog edge computing, IEEE Access 5 (2017) 5531–5538.

[90] K. Vohra, M. Dave, Securing fog and cloud communication using attribute based access control and re-encryption, in: 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), IEEE, 2018, pp. 307–312.

[91] Y. Yu, L. Xue, Y. Li, X. Du, M. Guizani, B. Yang, Assured data deletion with fine-grained access control for fog-based industrial applications, IEEE Trans. Ind. Inf. 14 (10) (2018) 4538–4547.

[92] C. Zuo, J. Shao, G. Wei, M. Xie, M. Ji, CCA-secure ABE with outsourced decryption for fog computing2, Future Gener. Comput. Syst. 78 (2018) 730–738.

[93] A.B. Amor, M. Abid, A. Meddeb, Secure fog-based E-learning scheme, IEEE Access 8 (2020) 31920–31933.

[94] X. Liu, Wei Chen, Yingjie Xia, Chenghan Yang, SE-VFC: Secure and efficient outsourcing computing in vehicular fog computing, IEEE Trans. Netw. Serv. Manag. (2021) SE-VFC: Secure and efficient outsourcing computing in vehicular fog computing, no. Ieee, 2021.

[95] A.S. Sohal, R. Sandhu, S.K. Sood, V. Chang, A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments, Comput. Secur. 74 (2018) 340–354.

[96] C. Li, Z. Qin, E. Novak, Q. Li, Securing SDN infrastructure of IoT–fog networks from MitM attacks, IEEE Internet Things J. 4 (5) (2017) 1156–1164.

[97] M. Davoodi, R. Moslemi, W. Song, J.M. Velni, A fog-based approach to secure smart grids against data integrity attacks, in: 2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), IEEE, 2020, pp. 1–5.

[98] P. Kumar, Govind P. Gupta, Rakesh Tripathi, Design of anomaly-based intrusion detection system using fog computing for IoT network, Autom. Control Comput. Sci. 55 (2) (2021) 137–147, Design of Anomaly-Based Intrusion Detection System Using Fog Computing for IoT Network, Springers:Automatic Control and Computer Sciences, 2021.

[99] Z. Li, X. Zhou, Y. Liu, H. Xu, L. Miao, A non-cooperative differential game-based security model in fog computing, China Commun. 14 (1) (2017) 180–189.

[100] D. Koo, Y. Shin, J. Yun, J. Hur, A hybrid deduplication for secure and efficient data outsourcing in fog Computing2, in: 2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), IEEE, 2016, pp. 285–293.

[101] P. Hu, S. Dhelim, H. Ning, T. Qiu, Survey on fog computing: architecture, key technologies, applications and open issues, J. Netw. Comput. Appl. 98 (2017) 27–42.

[102] J. Kang, R. Yu, X. Huang, Y. Zhang, Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles, IEEE Trans. Intell. Transp. Syst. 19 (8) (2017) 2627–2637.

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

[104] H.A. Al Hamid, S.M.M. Rahman, M.S. Hossain, A. Almogren, A. Alamri, A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography, IEEE Access 5 (2017) 22313–22328.

[105] R. Lu, A new communication-efficient privacy-preserving range query scheme in fog-enhanced IoT, IEEE Internet Things J. 6 (2) (2018) 2497–2505.

[106] K. Boakye-Boateng, E. Kuada, E. Antwi-Boasiako, E. Djaba, Encryption protocol for resource-constrained devices in fog-based IoT using one-time pads, IEEE Internet Things J. 6 (2) (2019) 3925–3933.

[107] K. Sarwar, Sira Yongchareon, Jian Yu, Saeed ur Rehman, Lightweight, divide-and-conquer privacy-preserving data aggregation in fog computing, Future Gener. Comput. Syst. 119 (2021) 188–199, Lightweight, Divide-and-Conquer privacy-preserving data aggregation in fog computing, Elsevier: Future Generation Computer Systems, 2021.

[108] M. Dong, K. Ota, A. Liu, Preserving source-location privacy through redundant fog loop for wireless sensor networks, in: 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, IEEE, 2015, pp. 1835–1842.

[109] R. Yang, Q. Xu, M.H. Au, Z. Yu, H. Wang, L. Zhou, Position based cryptography with location privacy: A step for fog computing, Future Gener. Comput. Syst. 78 (2018) 799–806.

[110] X. Yang, F. Yin, X. Tang, A fine-grained and privacy-preserving query scheme for fog computing-enhanced location-based service, Sensors 17 (7) (2017) 1611.

[111] M. Du, K. Wang, X. Liu, S. Guo, Y. Zhang, A differential privacy-based query model for sustainable fog data centers, IEEE Trans. Sustain. Comput. (2017).

[112] C. Zuo, J. Shao, G. Wei, M. Xie, M. Ji, CCA-secure ABE with outsourced decryption for fog computing, Future Gener. Comput. Syst. 78 (2018) 730–738.

[113] S. Basudan, X. Lin, K. Sankaranarayanan, A privacy-preserving vehicular crowdsensing-based road surface condition monitoring system using fog computing, IEEE Internet Things J. 4 (3) (2017) 772–782.

[114] L. Wang, G. Liu, L. Sun, A secure and privacy-preserving navigation scheme using spatial crowdsourcing in fog-based vanets, Sensors 17 (4) (2017) 668.

[115] B. Mukherjee, R.L. Neupane, P. Calyam, End-to-end IoT security middleware for cloud-fog communication, in: 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), IEEE, 2017, pp. 151–156.

[116] W. Fang, W. Zhang, J. Xiao, Y. Yang, W. Chen, A source anonymity-based lightweight secure AODV protocol for fog-based MANET, Sensors 17 (6) (2017) 1421.

[117] Y. Yao, X. Chang, J. Mišić, V.B. Mišić, L. Li, BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services, IEEE Internet Things J. 6 (2) (2019) 3775–3784.

[118] H. Wang, Z. Wang, J. Domingo-Ferrer, Anonymous and secure aggregation scheme in fog-based public cloud computing, Future Gener. Comput. Syst. 78 (2018) 712–719.

[119] N. Masaeli, H.H.S. Javadi, S.H. Erfani, Key pre-distribution scheme based on transversal design in large mobile fog networks with multi-clouds, J. Inf. Secur. Appl. 54 (2020) 102519.

[120] J. Liu, et al., Secure intelligent traffic light control using fog computing, Future Gener. Comput. Syst. 78 (2018) 817–824.

[121] C. Esposito, M. Ciampi, On security in publish/subscribe services: A survey, IEEE Commun. Surv. Tutor. 17 (2) (2014) 966–997.

[122] P. Hu, S. Dhelim, H. Ning, T. Qiu, Survey on fog computing: architecture, key technologies, applications and open issues, J. Netw. Comput. Appl. 98 (2017) 1–59.

[123] S. Das, A. Mukhopadhyay, D. Saha, S. Sadhukhan, A Markov-based model for information security risk assessment in healthcare MANETs, Inf. Syst. Front. (2017) 1–19.

[124] M.S. Alnaghes, F. Gebali, A Markov chain model for securing link layer in mobile ad hoc networks, in: 2015 SAI Intelligent Systems Conference (IntelliSys), IEEE, 2015, pp. 971–975.

[125] A. Patel, M. Taghavi, K. Bakhtiyari, J.C. JúNior, An intrusion detection and prevention system in cloud computing: A systematic review, J. Netw. Comput. Appl. 36 (1) (2013) 25–41.

[126] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Comput. Netw. 54 (15) (2010) 2787–2805.

[127] Y. Qiao, Z. Si, Y. Zhang, F.B. Abdesslem, X. Zhang, J. Yang, A hybrid Markov-based model for human mobility prediction, Neurocomputing 278 (2018) 99–109.