Journal of Reliable Intelligent Environments (2019) 5:209–233
https://doi.org/10.1007/s40860-019-00081-2

REVIEW

Security challenges in fog-computing environment: a systematic appraisal of current developments

Jimoh Yakubu[1] · Shafi'i Muhammad Abdulhamid[2] · Haruna Atabo Christopher[1] · Haruna Chiroma[3] · Mohammed Abdullahi[4]

Received: 13 January 2019 / Accepted: 22 April 2019 / Published online: 3 May 2019

Abstract

Fog computing is a new paradigm of computing that extends cloud-computing operations to the edges of the network. The fog-computing services provide location sensitivity, reduced latency, geographical accessibility, wireless connectivity, and enhanced improved data streaming. However, this computing paradigm is not an alternative for cloud computing and it comes with numerous security and privacy challenges. This paper provides a systematic literature review on the security challenges in fog-computing system. It reviews several architectures that are vital to support the security of fog environment and then created a taxonomy based on the different security techniques used. These include machine learning, cryptographic techniques, computational intelligence, and other techniques that differentiate this paper from the previous reviews in this area of research. Nonetheless, most of the proposed techniques used to solve security issues in fog computing could not completely addressed the security challenges due to the limitation of the various techniques. This review is intended to guide experts and novice researchers to identify certain areas of security challenges in fog computing for future improvements.

Keywords Fog computing · Fog-computing security · Cloud computing · Cloud-computing security · Fog-computing taxonomy · Edge computing

1 Introduction

Fog computing is a new model of computing that recently emerged to supplement the cloud-computing system. Its emergence is attributed to the increase in internet computation, web expansion, and complexity growth due to the increase of new technologies and solutions. The need for data processing and storage demands is also in astronomical increase. To address this phenomenon, Web architecture must be developed to meet user's data processing need [42]. Cloud computing has since been viewed as the main integration of internet system because of its computational and storage power that other computing devices does not possess [1].

However, the centralization of cloud services slows it down from providing timely response and mobility support which create lag between user request and cloud responses. For this reason, edge-computing concept emerged. Edge computing offers computational and storage capability just like the cloud, but are closer to the end user, where data are hosted or generated. The edge-computing model is a multi-tier architecture at the edge devices placed at the data centre [37]. Fog-computing paradigm is a new

✉ Shafi'i Muhammad Abdulhamid
shafii.abdulhamid@futminna.edu.ng

Jimoh Yakubu
jimm.yack@futminna.edu.ng

Haruna Atabo Christopher
christatabo@yahoo.com

Haruna Chiroma
freedonchi@yahoo.com

Mohammed Abdullahi
abdullahilwafu@abu.edu.ng

[1] Department of Computer Science, Federal University of Technology, Minna, Nigeria

[2] Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria

[3] Department of Computer Science, Federal College of Education (Technical), Gombe, Nigeria

[4] Department of Computer Science, Ahmadu Bello University, Zaria, Nigeria

concept developed to meet the latency requirement of this web architecture. The design greatly reduces latency and enhances network performance. The difference between fog computing and edge computing is in the computational power‘s location. Fog-computing computational power is located at the centre on fog nodes and internet-of-things (IoT) gateway.

Fog computing enables hosting of access points to the end-point devices at the edges. This allows various software and applications to be run closely to the data processing centre. The fundamental principle of the concept of fog computing is the edge technology which gives way to the smooth and convenience handling of data storage and computation close to the users at the network edge. Fog nodes possess various centralize interfaces close to data centre in the cloud to enable global coordination. Although the emergence of fog computing is still very new, this technology has already been embraced by the modern data centre and the cloud. The technology is built upon the distributed computing concept, such as content delivery networks, which ultimately allows the delivery of more complex services, using cloud technologies. Nonetheless, the distinguish features of fog computing from cloud are it nearness to the end user, since they offer computation, data storage, and provision of application services to the client. This does not in any way attempt to replace cloud computing with fog computing [46]. Rather, it is a perfect complement of many applications and services to eliminate the inadequacies of the cloud.

However, the fog paradigm inherits the security threats that are prevalence to the cloud computing. These threats expose the new platform to many security challenges that could negatively affect network and data. The impact of those security issues can jeopardize the flow of communication between the cloud, fog, and the edge devices. Therefore, protecting the fog communication network and providing maximum data protection in terms of confidentiality and integrity are a necessity to create secure fog environment. The previous researchers have proposed various techniques to solve the security issues in fog computing, but those techniques were not robust enough to completely provide security support and eliminate the challenges.

This proposed systematic literature review (SLR) paper will provides a comprehensive discussion on various security challenges in fog computing. The major objectives are:

- To systematically review latest papers on security challenges in Fog-computing environment based on range of time difference from the previous authors and the latest publications.
- To identify and exposed the gaps in the methods used in handling the various security challenges in the previous surveys.
- To guide the expert and the novice researchers the area of security challenges in Fog computing for possible improvements.

The remaining sections of this SRL are structured as follows:

Section 2 provides the basic concept of fog computing and the summary of similar-related survey, Sect. 3 describes the methodology applied in the review, Sect. 4 highlights the researches based on different security techniques, Sect. 5 summarizes the major research findings on security challenges in fog computing and data set analysis, Sect. 6 discusses the various sections of this paper, Sect. 7 points out some unresolved challenges and the future research work, and finally, Sect. 8 contains the conclusion of the SRL paper.

2 The basic concept of fog computing

This section presents the basic concept of fog computing for readers to understand the idea and how the fog computing operates. This can help novice researchers with interest to start research on security issues related to fog computing to understand the concept of the fog computing. In addition, expert researchers in other similar research areas intending to switch research focus to fog-computing security can use this as an initial reading material (Fig. 1).

Fog computing is the term used by Cisco to imply extension of cloud computing to the edge of an enterprise’s network. It can be perceived both in large cloud systems and in big data structures; this is evidence in the growing complexity in accessing information objectively [45]. Fog computing facilitates the operation of computation, storage, and networking services between end devices and cloud-computing data centres. While edge computing is typically referred to the location, where services are instantiated, fog computing implies distribution of the communication, computation, and storage resources and services on or close to devices and systems in the control of end users.

Fog-networking complement IoT operations and most of the devices on the network are connected to each other. The features of fog computing include: edge location, location awareness, and low latency. Others are large number of nodes, large-scale sensor networks, real-time interaction, predominance of wireless access, and support for mobility [51]. Utilizing Fog computing when there is no real use case can be a burden rather than solving a problem [27]. To that end, there are ways in which fog computing can be absolutely applicable so as to enjoy the benefit of fog-computing technology. Increase in data processing and delivery efficacy, bringing data close to the user, support for mobility and the IoT, reduces network

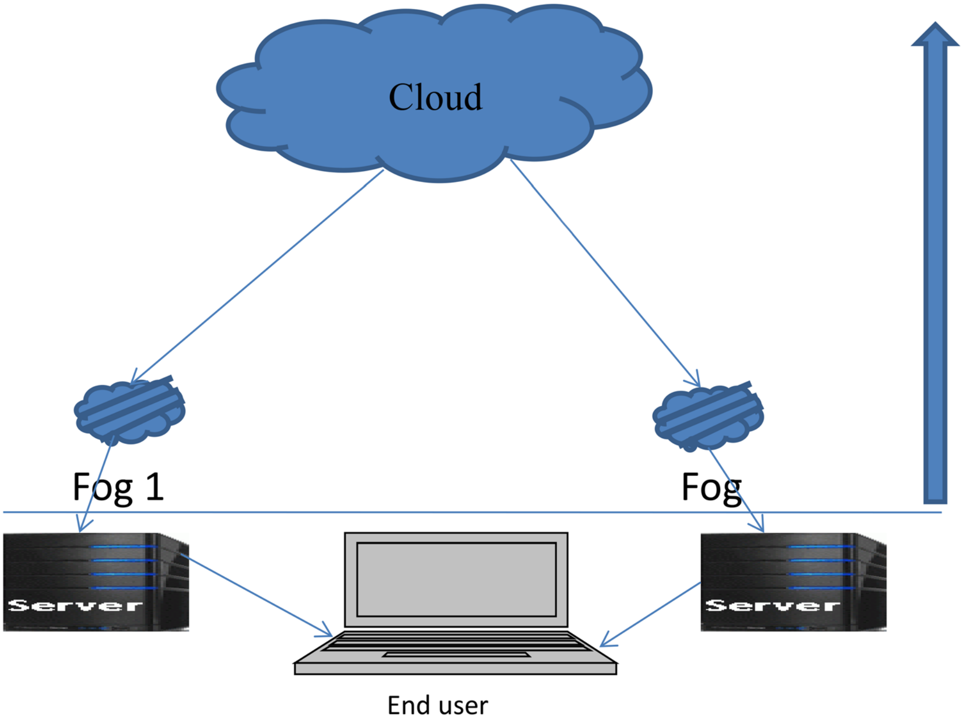

Fig. 1 Architecture of fog computing

Table 1 Differences between the cloud and the fog

Cloud	Fog
Centralized architecture	Decentralized architecture
Average scalability	High scalability
High latency	Low latency
Service access (through core)	Service access (at the edge)
Service availability (high)	Service availability (high)
Explicit mobility (not possible)	Explicit mobility (possible)

congestion, boast some impressive scaling abilities and possible integration with the cloud, and other services.

In spite of all the numerous benefits, there are still some drawbacks which if not carefully thought of may negate the operation of fog computing; it adds more complexity into a network, and consequently increases certain amount of overhead commercially. Implementing fog-computing technology introduces more number of points of failure. Several quantities of data are presently being distributed to more users to optimize the concept of the cloud. Organizations and data processing centre need to find a medium to deliver contents to end users through a more centralized distributed platform. The idea of fog computing is to distribute data to move it closer to the end user to remove latency and numerous hops, and support mobile computing and data streaming. The differences between the fog computing and the cloud-computing systems are summarized in Table 1.

2.1 Previous surveys conducted on security issues in fog computing

This section presents the previous surveys conducted by researchers in security issues regarding fog computing. The surveys are pointed out for readers to understand the difference between the surveys already published and the current survey presented in this paper. The security issues in the fog computing is attracting serious attention from the academia which led to the emergence of ten different surveys in the literature. For example, Bilal et al. [6] identified the various potentials, trend, and edge-computing challenges. This paper surveyed fog computing, cloudlet, microdatacenters, and mobile edge. Despite the differences in the mentioned technology, the researchers observed that the technologies are structured to achieve the same purpose which most importantly is to bring data and information closer to the end users. The team pointed out that most of the challenges faced by the new technology are due to the non-standardization of edge technologies. Furthermore, resource management and allocation, general purpose computing in edges, security, and privacy are considered as major challenges faced by edge computing which inhibit the development and adopting of edge computing. Lack of standard and realistic design is said to be contributing factor to the challenges encountered by the edge computing. Similarly, the team asserts that increase in computation will lead to proportional increase on the load of the server. Suitable resource management and allocation was suggested as the major task to overcome the challenges. To maintain reasonable level of quality of service, fault tolerance and automatic recovery from fault are said to be important factors to be consider especially in a real-time application such as edge. Furthermore, this paper suggested the inspection of peak hour usage of edge nodes by deploying effective monitoring mechanism. However, there is need to integrating a billing model that may generate maximum revenues at service provider's end (Table 2).

More so, detailed analysis of the security of edge paradigms was provided by Roman et al. [38]. The team analyses most pronounced characteristics and the differences among them with their challenges and potential synergies. The research indicated that attention of the previous researchers on the security mechanism only focused on one particular edge paradigm without the thought of adapting and extending it to other security mechanisms. The researchers figured out mobility and network architecture as conspicuous examples of similarities between all paradigms. It emphasized that all paradigms pursue the creation of federated infrastructure in which most of the edge infrastructure coexist to exchange information and services. Scalability of the ecosystem, having access to information, low and predictable latency and packet delay variation are the likely benefit of federated infrastructure. This paper enumerated the major challenges that are common to edge paradigms among which are: infrastructure, virtualization, resources task, distribution, mobility, and programmability. The research identified VMS management as basic area of clear synergies between paradigms. Nevertheless, the researchers could not evaluate certain impact that attack such as denial of service, rogue data centre, and some malicious VMs may have on the service infrastructure.

Table 2 Acronyms and their meanings

Acronyms	Meanings
IoT	Internet of things
VM	Virtual machine
URL	Uniform resource locator
VMS	Virtual managed services
IEEE	Institute of electrical electronic engineers
SDN	Software-defined networking
MAC	Medial access controller
PKI	Public key infrastructure
ACM	Association of computing machine
GMT	Greenwich mean time
AES	Advance encryption standard
API	Application programming interface
MITM	Man-in-the middle
CPU	Central processing unit
SRL	Systematic literature review
CIA	Confidentiality, integrity, availability
MBD	Mosquito-borne diseases
TNA	Temporal network analysis
EWS	Early warning score
ABE	Attribute-based encryption
SDS	Software define system
SbSBP	Security-based service broker policy
CP-ABE	Cipher-text policy attribute-based encryption
KP-ABE	Key-policy attribute-based encryption
DCs	Datacenters
HPCS	Hybrid privacy-preserving clinical decision support system
QIP	Quantum information processing
MCSS	multi-cloud storage systems
FSDR	Fog-computing enabled secure demand response
SSL	secure sockets layer
DCF	Distributed coordination function
NFV	Network function virtualization
DOS	Denial of service

Furthermore, trust model reputation that is based on solution to e-commerce, peer-to-peer (P2P), and online social networks was identified in a survey conducted by Yi et al. [55]. The authors described the distributed polling algorithm as veritable tool to address trust and authentication issues to ascertain reliability of source before downloading. The review identified fake fog node as the main threat to data security and privacy. To prevent the connection of client to rogue access point, the review indicated that measurement-based method proposed by Han et al. could address the challenges of fake fog node. More so, the review shows that data storage security can be tackled through auditable data storage. Nonetheless, while the implementation of SDN techniques helps in securing fog network, this paper observed that certain security risk also emerges as new challenges. Conclusively, the team specified the combination of searchable encryption and holomorphic encryption as the best alternative to securing the integrity, confidentiality, and availability of data storage. However, the reviewer could not expose the vulnerability of fog-computing attacks.

Insecure authentication protocols were identified as the major security threat to fog-computing platform and the end-user application devices. The IoT devices especially in smart grids is expose to data tempering and spoofing attack which can ultimately be prevented using infrastructure, intrusion detection techniques, and Hellman key exchange. Video call investigation between 3G and WLAN user within a fog network was conducted for man-in-the-middle attack which result shows that the attack did not reveal obvious changes in the memory utilization and CPU consumption of fog node. In addition, Authentication scheme through securing communication channels between the fog environments was suggested by the authors to be adopted as preventive measure. Similarly, advanced encryption standard (AES) was also recommended as a viable encryption techniques for fog platform [18]. Conversely, the security solutions put forward by the team are individualistic and, therefore, not dynamic enough to secure fog platform in terms of confidentiality, integrity, and availability.

Similarly, the security of fog architecture that is based on techniques and security threats was investigated by Abbasi and Shah [2] in which the team classified fog architecture into first tier, second tier, and the third tier. The first tier is the end user such as devices, other IoT objects, and application devices. The second tier executes anomalies and other different tasks by breaking it into sub levels. The third tier consist of cloud data centres which handle policy definition, decision making in a long term, disaster management, and scheduling of greater task. Furthermore, the researchers enumerated the security techniques which were proposed in the past to resolve all the security challenges. Authentication and authorization remain the foremost security techniques. Others are network security, access controls mechanism, intrusion detection (IDS), privacy, building and managing trust, virtualization, forensic, fault tolerance, and recovery. More so, this paper highlighted the architectural loopholes, where security challenges can be detected. Service infrastructure networks and virtualization and user devices are the existing security that can be identified. This paper suggested the hybrid of the security techniques to enhance and improve the security of fog-computing environment. However, this paper does not consider other attacks which could maliciously hinder the data security.

Hu et al. [14] surveyed and review the architecture, key technologies, application, challenges, and open issues in relation with computing technology. The authors compared and differentiated fog computing from the cloud. The main technology for computing includes computing, communication, and storage technologies, naming, resources management, security, and privacy protection. These technologies enable fog computing to influence more smart and adaptive services rendered to the users. Security and data protection was said to be the vital area that necessitate the development of fog to prevent malicious attack. More so, the researchers described fog computing as a conducive medium for application with low latency requirements. Health care, cyber-physical system, and urgent services are the areas fog computing can be applied. This paper concluded that several system security problems are still encountered by the fog devices out of protection and surveillance range. Nevertheless, the survey did not identify the various attacks that contributed to the security problems.

Access control is considered to be a veritable tool to secure and control access to fog-computing environment efficiently. Access-control requirements which include latency, efficiency, generality, aggregation, privacy protection, resource restriction, and policy management were classified by Zhang et al. [57]. This paper further group access control into model which are as follows: discretionary access-control (DAC) model, mandatory access-control (MAC) model, role-based access-control (RBAC) model, attribute-based access-control (ABAC) model, usage-control-based access-control (UCON) model, and reference-monitoring access (RMAC) model. Nonetheless, none of the mentioned access control can address all the existing security threats.

Roman et al. [38] highlighted the common challenges in edge paradigm that the various security threats and challenges can maliciously affect. These include infrastructure, virtualization, resources and task, distribution, mobility, and program ability. The researcher stressed the need of greater collaboration among several edges datacenters that operate and of standards which specify the way that the various architecture elements can be harmonized and collaborated with each other to pave way to information access to virtual machines. More so, this paper enumerated certain attack that can be launched against assets of edge paradigms, denial of service (DoS), man in the middle, rogue gateway, service infrastructure, VM manipulation, injection of information, service manipulation, and user devices which are considered as possible attack on the asset of edge computing. The team emphasized the need of data centres and administrator to make use of security protocols and extensions that will be used for such technologies for implementation. To maintain defense against different threats, this paper suggested deployment of various types of security services and mechanism such as identity and authentication, access-control system, protocol and network security, virtualization, and fault tolerance and resilience. Nevertheless, the impact of the mention attacks could not be established by the authors.

Lisbon and Kavitha [24] classified cloud and fog security threats into data issues, network issues, and environment issues. The authors critically examined data breach, data lose, and the number of data threat occurrences between 2005 and 2016. The team opined that adapting decoy technique at the fog layer is key to preventing data breach threat. Data backup and data recovery techniques are said to be an important method to avoid threat at the cloud and fog level. To address the network issues, multi-level authentication and intrusion detection at different levels are needed to avoid account hijacking and denial of service. Weak APIs were attributed to the major cause of insecure interface and APIs which make the third party gains access to information in the cloud. However, this paper was unable to address fog solution for insecure interfaces, shared technology vulnerability, and insufficient due diligence. Conclusively, the researchers emphasized that there is no feasible fog solution to environmental issues presently. This was attributed to the infant development stage of the fog computing.

Shirazi et al. [41] investigated models and architecture of extended cloud and the technologies to implement them.

Anomaly detention and policy-based resistance management are suggested to be key to improvement of security and resilience achievement in the environment of extended cloud. This paper pointed out several threats which include location exposure, insecure management, distributed images of vital machines, jamming attacks, and weak authentication as the possible threats to edge and fog and invariably poses serious security risk to the cloud. The authors emphasized that security and resilience are vital issues to be considered in mobile edge computing (MEC) with privacy of shared data in MEC facilities. Similarly, the team observed that end-to-end security is another key requirement for fog model applications. They recommended the inclusion of better integration of privacy, security, and resilience to protect MEC mechanism. More so, the authors call for standardization of the fog architecture that could lead to better computing. Conversely, this paper lacks explicit concept of MEC to clearly address the designing of MEC framework. The summary of the survey discussed in this section is presented in Table 3.

3 Systematic review methodology

In this review, Kitchenham et al.'s [19] method of literature review was adopted and the duration for the search was between 20th December, 2017 and 27th December, 2018. To execute this review process, the following procedures was adopted: research questions, research strategy, and selection criteria.

3.1 Research questions

In the course of this review, three research questions were asked:

1. What are the security challenges in fog computing?
2. What are the existing methods/techniques used to address the security challenges?
3. What security and challenges gaps needed to be addressed?
4. What are the data set used?

3.2 Research strategy

Various famous academic databases were used to identify and retrieve literature (conference proceedings, journal articles and edited book chapters) for the SRL.

3.3 Data source

The databases used for the literature search involve ACM Digital Library, Springer link, Science direct, Web of Science, DBLP, Scopus, Google Scholar, IEEE Xplor^{tm}, Taylor and Francis, and Citeseerx. These academic databases were used in conjunction with some criteria that are used to evaluate the result. The academic database used for searching the journal is represented in Fig. 2.

3.4 Selection criteria

The selection and the procedure for elimination are shown in Fig. 3. The focus was based on survey and research journal/article that the subject matter is directly related to security challenges in fog computing. In this study, the selection criteria include all identified papers, screened exclusion by title, screened exclusion by abstract, screened based on full-text content eligibility, and the included papers that are relevant to the review. The total search result is 417. Out of the search total, 398 papers were sieved based on duplicate papers, 224 based on title exclusion, 98 based on abstract extraction, 58 on the basis of full-text eligibility, and finally 52 on the basis of included relevant studies.

Table 3 Summary of related survey

S. no.	References	No. of references cited	Range of time	Latest reference
1.	Lisbon and Kavitha [24]	26	2010–2017	2017
2.	Khan et al.[18]	149	2011–2017	2017
3.	Bilal et al. [6]	170	2011–2017	2017
4.	Roman et al. [38]	132	2010–2016	2016
5.	Yi et al. [55]	49	2012–2015	2015
6.	Hu et al. [14]	124	2013–2017	2017
7.	Zhang et al. [58]	12	2011–2017	2017
8.	Shirazi et al. [41]	57	2011–207	2017
9.	Abbasi and Shah [2]	20	2011–2017	2017
10.	Mahmud et al. [29]	47	2013–2016	2016
11	This review	57	2013–2018	2018

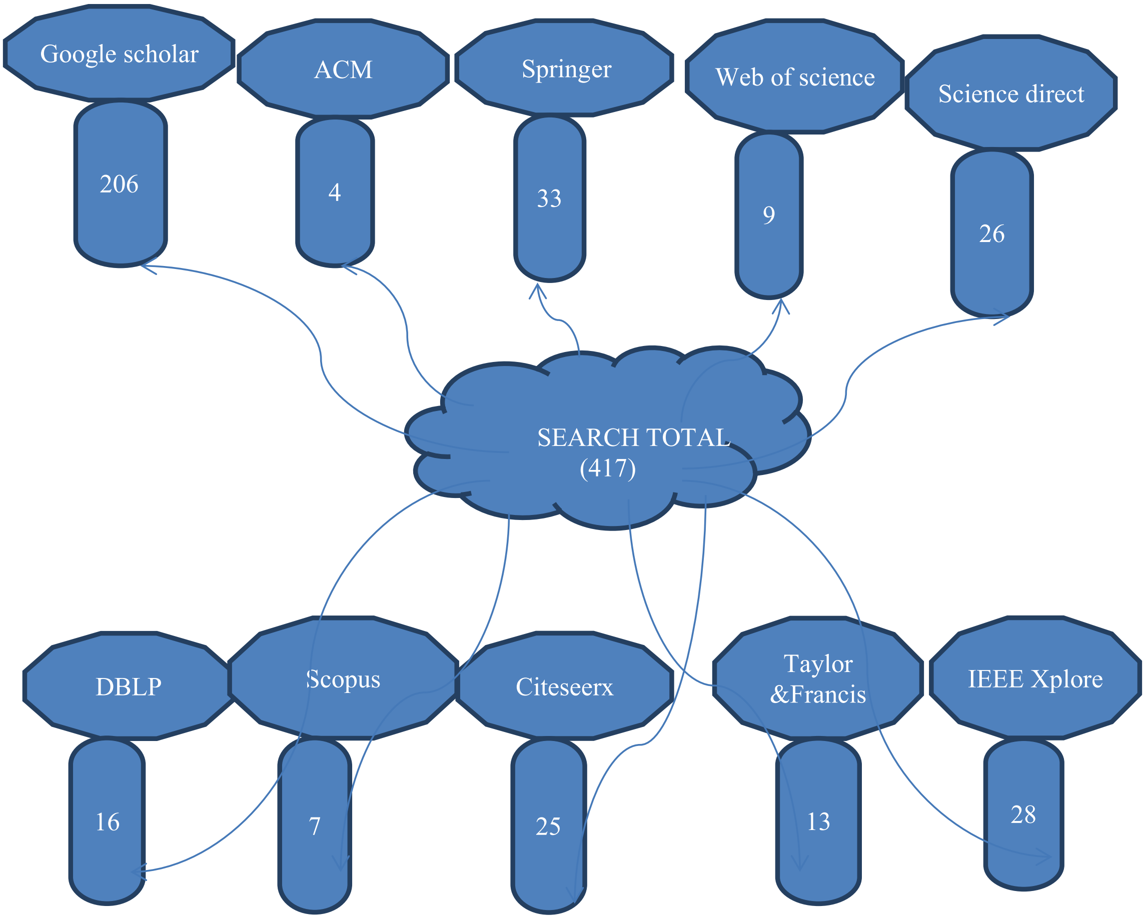

Fig. 2 Academic database used for searching the journal

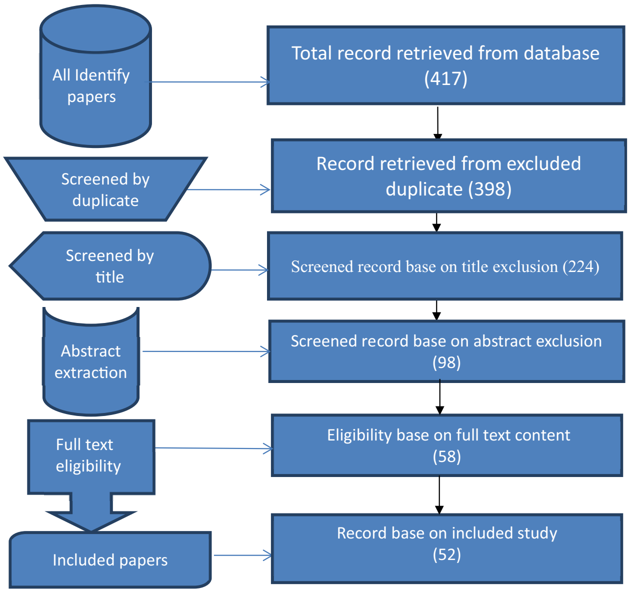
All Identify papers
Total record retrieved from database (417)
Screened by duplicate
Record retrieved from excluded duplicate (398)
Screened by title
Screened record base on title exclusion (224)
Abstract extraction
Screened record base on abstract exclusion (98)
Full text eligibility
Eligibility base on full text content (58)
Included papers
Record base on included study (52)

Fig. 3 Study paper selection criteria diagram

3.5 Inclusion and exclusion criteria

- Inclusion criteria
  - This includes papers that analyze fog-computing architecture.
  - Papers whose study is writing in English language.
  - Papers that focused on presenting the present security challenges in fog computing.
  - Journals/article that are survey or research papers.
  - Accessible published papers from 2012 to 2018.
- Exclusion criteria
  - Study paper that is not written in English language.
  - Papers that are mainly about cloud computing.
  - Papers that are not survey nor research.
  - Inaccessible papers.

The pie chart representation of data source is represented in Fig. 4

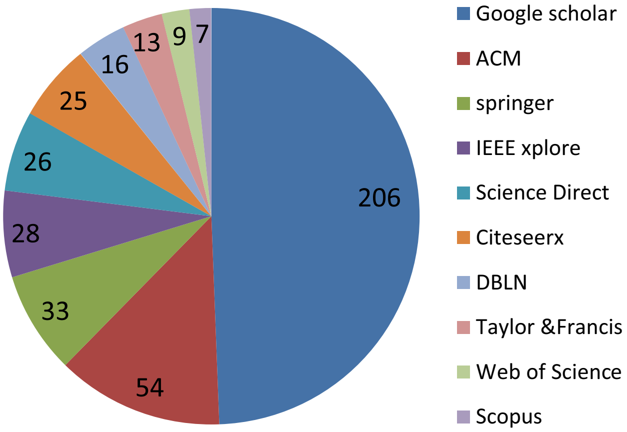

Fig. 4 Pie chart representation of data source

4 Research based on different security techniques

Figure 5 shows the new taxonomy created based on the review conducted. The taxonomy is created according to the security techniques found in the fog-computing literature.

4.1 Cryptographic techniques

Sharma et al. [40] proposed a novel block chain-based distributed cloud framework with software-defined network (SDN). The model is a distributed cloud infrastructure that can provide low cost, secure, and on-demand access to the most active computing infrastructures in an IoT network. The technique is efficient in terms of cost effectiveness and high-performance computing. The researcher's result shows improved response time, reduces delay time, and has the ability to detect real-time attack on an IoT network. Energy-harvesting techniques for energy efficient communication in the device on the IoT network are considered as future direction. However, more evaluation is needed to prove the effectiveness of the new scheme.

The construction of secure positioning protocol with privacy, in the bounded retrieval mode, was presented by Yang et al. [53]. In the said mode, the team described the possible ways to protect location privacy of the position prover in which its position is based on cryptographic protocols. The authors considered one-dimensional case and three-dimensional case in the construction of the protocol. While the one-dimensional case supports the claim region of any interval between two protocols, the three-dimensional case

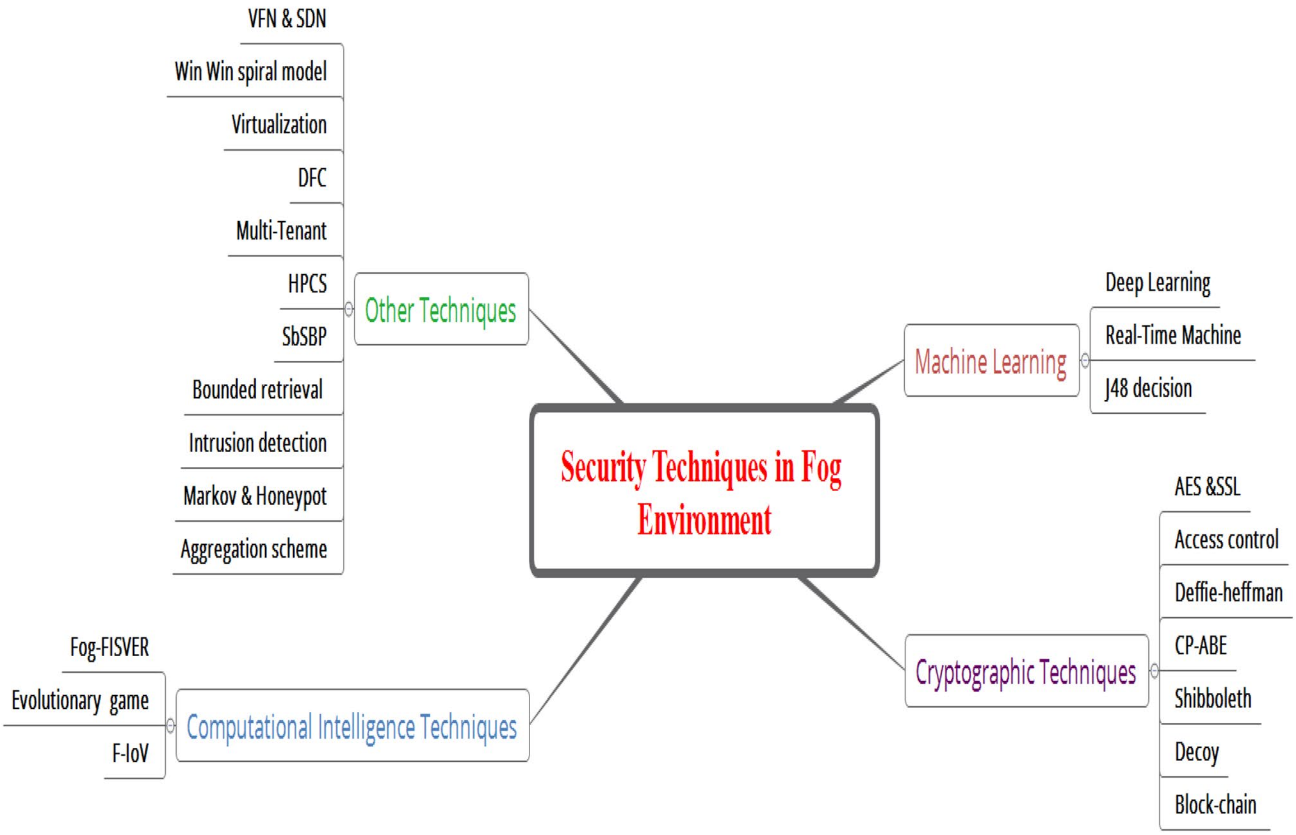

Fig. 5 Taxonomy of security techniques in fog-computing environment

supports only a claim region of some specified shapes. However, the retrieval mode cannot address other regions in the bounded mode.

An efficient access-control scheme with outsourcing capability and attribute update for fog computing was proposed to remove the burden of encryption and decryption, and the outsourcing techniques were used in conjunction with the fog nodes. The research revealed less cost of computation generation as well as secure scheme in terms of security. The proposed scheme is said to be efficient and effective techniques that can be employed in the computing activities [57, 58]. However, the new scheme cannot address all access-control problems.

Zahra et al. [56] deployed Shibboleth protocol into the cloud IoT network, to secure data access and outsourcing. The scheme can efficiently manage security and access which ensures security between fog client and fog nodes. Using HLPN, the effectiveness of Shibboleth against some security features was established. The experimental result indicated that some security features accepted shibboleth protocol as better method in achieving highly protected security. Conclusively, the authors viewed the deployment and integration of shibboleth protocol as a better security mechanism to respond to the general security of the IoT network. Conversely, this paper does not point out the types of security threats that are best controlled by the security scheme.

Flexible IoT security mechanism for end-to-end cloud–fog communication to address the security of the network that is located at the user fogs [32]. The proposed system provides intermittent security and resource-aware security especially for smart devices and other application that hosted the cloud. The result shows that static pre-share keys (PSKs) can effectively fast track secure communications. Similarly, the result indicated that it is possible to find useful alternative among the various security methods which required an optimal scheme decider developed by the team. The optimal scheme decider has the ability to use a security scheme database to source and use optimal security scheme to solve constraints problems. Nevertheless, the researcher does not conduct indebt evaluation to show the extent of security control of user fogs, since the present system cannot address all fog security problems.

Novel CP-ABE techniques that protect any form of key-delegation abuse were proposed by Jiang et al. [16]. It is a cipher-text policy scheme that is attribute-based encryption which makes users not to generate new private keys of a subset of the user's original sets of attribute without authorization. The new scheme is intended to correct the key-delegation abuse suffered by ABE system. While the techniques are said to be more efficient in terms of attribute arrangement, it can also effectively traced the possible violators. However, the CP-ABE scheme needs sufficient investigation to ascertain the level of support for other access structures.

Wang et al. [48] proposed the notion of anonymous and secure aggregation scheme (ASAS) in fog-based public cloud computing. The new scheme gathers the data from terminal nodes and sends the aggregated data to the public cloud server. Bilinear pairing and Castagnos–Laguillamie cryptography were used to verify the model. The authors observed that ASAS scheme save bandwidth between fog nodes and the public cloud. Similarly, the computation time of the public cloud is conserved. The result of the security performance evaluation shows that the model is secure and highly efficient. Nonetheless, the security notion cannot all attack problems.

Xiong et al. [52] proposed a model that is capable of preventing different types of attacks from cloud and fog vendors. The technology uses fog and cloud to store various data types and also keeps their relationships which remove different security challenges in the cloud architecture. Message authentication code (MAC) is used to compute data on encrypted data scheme through advanced encryption standard (AES) and secure sockets layer (SSL). The framework makes it easy for key management processing of cloud. The scheme ensures data validation and prevents encrypted data from being corrupted. The authors utilizes fog-computing scheme to provide additional privacy, flexibility, and easy access. The result of the tested scheme shows more secure system and lesser time needed to access encrypted data. Nevertheless, in spite of the combined security parameter, more evaluation needs to be conducted to determine its efficiency in handling man-in the-middle attack scenario.

El-Latif et al. [10] also proposed security mechanism based on quantum stenography architecture to secure the flow of messages in fog cloud IoT. The framework enables both the user at a particular location to append their useful data through the protocol and the intended receiver in another location to have access to the data in transition in the fog cloud. The content of the transient messages is being retrieved through the proposed approach. The authors employ hash function to authenticate the secret messages in transition. More so, the dynamism of the proposed system proved that the security architecture is secured against some visible attacks. However, the memory utilization and CPU consumption rate are not being investigated by the team.

In the study conducted by Shropshire et al. [42] to figure out, potential weakness before embarking on development of software focus is on integrity, confidentiality, and availability (CIA) to address the security issue of the intended infrastructure. The platform combined virtualized network with hardware and software functionality into a unified single unit. The result of the developed infrastructure provides support for virtual machine that can interpret the combined infrastructure. The author explained further that the integrated structure resulted in service improvement, but at the end-user position, and the transport layer communication between the fog node and the cloud can be intercepted at the end node. Furthermore, the study concluded that in the view of the security consequences of CIA, effort should be focused on high-level design development. Integrated virtualization layer and the extension of the management backplane to the edge of the network are identified by the author as the simplified paradigms that will pave way for communication among various distributed machines. However, the research could not cover the specific analyses to identify fog-computing weakness.

Koo and Hur [20] proposed a secured data deduplication framework that is efficient in management ownership in fog computing. The team secured fine-grain access control through user-level management update efficiency for outsources data which enable cryptographic access-control enforcement. The proposed scheme ensured consistent privacy through updating user-level public keys and cipher text. The result of the scheme shows significant reduction of communication level and the number of keys without necessary causing security degradation. Nevertheless, the new system is highly dependent on user-level public keys update without which, security will be degraded.

Fu et al. [12] designed a secure, flexible, and efficient storage and retrieval architecture that integrated the fog- and cloud-computing methods. The authors developed a retrieval tree to support accurate data retrieval and index encryption techniques that are based on KNN algorithm to back the policy-preserving data search. The experimental results validate the significance of the new scheme and the efficiency, which improved the security of the stored data and retrieved the same in industrial internet of things (IIoT). However, the designed scheme is not robust enough to handle multiple data retrieval which could have supported the users greatly. Table 4 presents more details.

4.2 Machine-learning techniques

A novel distributed deep-learning model for driving fog-to-thing-computing attack detection scheme which is an improvement over classical machine-learning attack detection was proposed by Ebebe and Naveen [9]. The authors subjected the experimental setup to NSL data set in which the result shows that the proposed deep-learning models are capable of accuracy detection, false alarm rate, and scalability when compared with shallow models. Nevertheless, more investigation and evaluation of the designed model is needed on different platforms to determine the efficiency and performance of the new scheme using different data sets.

Huang et al. [15] showcased architecture for vehicular fog computing and also presented a specific use case that exists in vehicular fog computing. The vehicular fog-computing model in conjunction with traffic-scheduling algorithms is expected to remove the problems faced by various vehicular applications. By aggregating the data, filter the data before uploading. The said method pre-processes the data collected and will eventually resolve the issue of too large data communication over vehicular applications. The authors also present security and forensic challenges and solutions. Conversely, the vehicular fog model is limited by authentication efficiency and revocation cost. Singh et al. [43] developed a framework for cyber security that basically uses three technologies which are two markov model, intrusion detection system (IDS) as well as virtual honey pot (HVD) to detect malicious edge devices in fog-computing environment, while the hidden markov model effectively categorized the VHD designed store and keeps the maintenance of log repository of all the detected malicious devices which defend it from unknown attack that could be launched. The experimental result shows that the proposed method is capable of solving all issues related to edge device attack. Integration of the proposed framework with lager ethical hacking and penetration services from cloud framework was suggested as future direction which will ensure the robustness and resilience against attack and hacking activities. On the contrary, the team did not experiment with wider ethical hacking activities to measure the resilience and dynamism of the proposed techniques.

Donovan et al. [8] deployed fog computing to establish real-time embedded machine learning for industrial 4.0 design operation. The author’s findings revealed the capability of fog to generate constant and more reliable cyber-physical interactions for real-time engineering problems that are fault tolerant. The proposed techniques can also protect data security and privacy by making sure that the execution of data are enclosed within the physical boundaries of the facilities. The team recommends the use of hash-based authorization scheme to discover and harmonize system as future direction. On the other hand, this paper does not put into consideration, the deployment of physical devices within the factory, which will enhance distribution of work to the nodes to scale the resources.

A system that is based on IoT sensors, fog, and cloud computing to differentiate and classify and to keep surveillance of the users who were infected with mosquito-borne diseases (MBDs) was presented by Sood and Mahajan [44]. The main purpose of the novel system is basically to control the possible outbreak of MBDs at infant stage. The fog–cloud-based cyber-physical system proposed by the researcher used similarity factor to make distinction with reference to the symptoms to detect MBDs, and then, the fog layer generates alert messages to serve as notification and warning to the users. The classification of users based on category was done through J48 decision tree alongside with the temporal network analysis (TNA) which monitors

Table 4 Analysis of cryptographic techniques

S. no.	References	Proposed technique	Problem addressed	Comparison methods	Major findings	Parameter used	Limitation
1.	Zahra et al. [56]	Intrusion detection technique in combination with Hellman key exchange	Man-in-the-middle attack (MITM)	Not state	Attack does not cause significant change in Memory and CPU consumption of fog node	Processor usage (CPU) and memory utilization I/O rate	Suggested security solutions are insufficient enough to protect the fog platform against CIA
2.	Fu et al. [12]	Retrieval tree and index encryption techniques with KNN algorithm	Privacy-preserving data search	Not stated	Improved storage data security and retrieval in IIoT	Not disclosed	The new scheme is not robust enough to handle multiple retrieval
3.	Koo and Hur [20]	Secured data deduplication scheme	Consistency in privacy through user- level public key and cipher text	Secure data deduplication using fixed shared key	Reduction of communication level and number of keys without security degradation	Not disclosed	The new technique is highly dependent on user-level public keys update
4.	El-Latif et al. [10]	Quantum steganography	Securing of flow of messages in fog and clout IoT	Quantum information processing (QIP)	Secured architecture against visible attack	Not stated	Memory utilization and CPU consumption is not investigated
5.	Sharma et al. [40]	Block chain-based distributed cloud framework	Reduce delay time, real-time attack detention	Core-based cloud-computing infrastructure	Secure and improved response time and on-demand access with low-cost	Not stated	More investigation is needed with respect to memory utilization of the scheme
6.	Zahra et al. [56]	Shibboleth protocol	Data and security access management	Digital signatures	Better security mechanism	Not state	The authors did not highlight the types of security threat that is best controlled by Shibboleth scheme
7.	Jiang et al. [16]	CP-ABE in conjunction with KP-ABE	Protection of key-delegation abuse	CP-ABE	More efficient in attribute arrangement	Not stated	No established investigation to determine the level of support of the scheme for other access structure
8.	Zhang et al. [57]	Decisional bilinear Diffie–Hellman	Removal of encryption and decryption bottleneck	CP-ABE	Secure scheme and less cost of computation	Not disclosed	This paper did not highlight the security type that is control by the scheme
9.	Wang et al. [48, 50]	Anonymous and secure aggregation scheme	Bandwidth and time conservation	Pseudonyms technique	Highly efficient and secure model	Not disclosed	The security notion cannot dynamically address all attack threats
10.	Xiong et al. [52]	AES and SSL	Prevention of unauthorized access to information	Cryptographic parameters	Secure and effective way to prevent attacker to access unauthorized information	The average time required for the security level and the search for data	The combined security parameters cannot address man-in-the-middle attack

and shows the present condition of MBDs outbreak through data that are nearer. The result of the experiment projected high-performance rate for differentiating the MBDs. However, the proposed system lacks the capability to quarantine the detected MDBs at early stage. It can only differentiate and classify MDBs. Yaseen et al. [54] developed fog-based model that can be exploited for real-time monitoring and detection of collusion attacks in IoT environment. The team-integrated software-defined system layer (SDS) that can retrieve various types of data and then discover all the other types of attacks apart from collusion attack. To ascertain the reliability of the system, the authors designed an algorithm, theorem, and proofs that established the authenticity, correctness, and scalability of the framework. The experimental result shows distinction between wireless sensor networks and the proposed system. The later is capable of tracking malicious nodes moving from one point to another in IoT environment in deviation from the former. However, the model lacks authentication system that will reduce instances of collusion intruders. Table 5 shows the analysis of the machine-learning techniques.

4.3 Computational intelligence techniques

An advanced framework over FISVER that is used for smart transportation safety (STS) was proposed. The improved system called Fog-FISVER is a three-tier architectural design and incorporated in vehicle for intelligent public safety in vehicular environment [34]. The framework integrated fog-computing idea with smart video surveillance in smart transportation system to assist crime detection that is sufficient, but costless in a real time on public bus services. The result of the tested new prototype was observed by the team to perform better with higher efficiency and also overcomes the limitation of the earlier version of the prototype. Conversely, more study and evaluation of the improved framework is yet to be done to assess the impact of the new system on the rate of crime detection and timely notification of mobile application.

Sun et al. [47] employed fog-computing paradigm to propose security mechanism that is based on human nervous system. Evolutionary game theory was used by the authors to perform mathematical modeling and analysis. The result indicated that the proposed method is capable of reducing the number of attack behaviour efficiently. The team also evaluated novel techniques and concluded that while profit of users is on the rise, the overall security mechanism of the system is maintained and enhanced. Nonetheless, this paper did not specify the types of attack and behaviour pattern, since attack comes in various forms and method, as shown in Table 6.

4.4 Other techniques

Wang et al. [49] proposed a fog-based cloud storage scheme on fog computing. The scheme provides data privacy which ensured integrity, availability, and confidentiality of user's data. In the proposed scheme, data are stored both in the cloud and in the fog which can also be retrieved from both separately. The scheme is capable of preventing user's data from possible cyber attack which could lead to data loss and modification of any such. This is made possible by dividing the user's data into two parts, such that that the big part is the cloud and the other small part in the fog server. The team developed an easy-save architecture, whose evaluation shows feasibility and efficiency. The result of experimental setup proved that the rate of transmission between the fog server and user's device is faster than the transmission rate between the cloud server and the user's device. However, the novel scheme is not subjected to man-in-the-middle attack to determine the stealthy nature of the attack.

A hybrid privacy-preserving clinical decision support system (HPCS) in fog and cloud environments that are capable of monitoring and predict diseases for patience health status was presented by Liu et al. [25]. The authors used inner product protocol to achieved lightweight single-layer neural network in fog to tackle five major challenges of fog- and cloud-computing architecture which includes: basic real-time and high-accuracy classification to monitor patient's health condition in real time, secure data storage, and prediction which assist diagnosed patient illness, secure non-linear function processing which is capable of performing non-linear functions privately. Other challenges tackled by the researchers through the hybrid system is the support iterative calculations that enable unlimited calculation task repeatedly and also the ease of use that enables patient to query the server and gets response from either fog or cloud in timely manners. Cancer Wisconsin repository was used to test the HPCS in which the experimental result through neural network indicated monitoring of patient health status without unauthorized user interference. However, the proposed technique is not capable of monitoring emergency situation, especially the case of accident victim.

Fog-computing supported IoV called F-IoV that utilizes resources at the edge of the network for proper management of pseudonym to address location privacy challenges was proposed. Pseudonym fogs are deployed in road infrastructures that are nearer to the vehicle. The introduction of p^3 scheme in F-IoV shows that the p^3 framework improved secure communication and privacy preservation for vehicle [17]. Nevertheless, the proposed scheme only applicable to cluster vehicles, but cannot dynamically handle other cases with sparse vehicles.

Intel Edison as mist and fog computers to develop SoA Mist framework was proposed in Barik et al. [4]. The

Table 5 Analysis of machine-learning techniques

S. no.	References	Proposed technique	Problem addressed	Comparison methods	Major findings	Parameter used	Limitation
1.	Huang et al. [15]	Forensics	Reduction of road traffic congestion and car accidents	Not stated	Real-time identification, collection, and analysis of data	Not stated	Forensic requirement presented cannot address all available security threats
2.	Ebebe and Naveen [9]	Deep-learning algorithm (DL)	Cyber-attack detection	Shallow algorithms	Improvement on the accuracy and efficiency of cyber-attack detection	Not stated	The authors did not verify the scheme using different data sets
3.	Singh et al. [43]	Markov model and virtual honey pot	Detection of malicious edge devices in fog environment	Honeypot	Maintenance of log repository and defend it from unknown attack	Not stated	The authors did not investigate wider ethical hacking activities
4.	Donovan et al. [8]	Real-time embedded machine-learning application	Data protection security and privacy	Industrial cyber-physical systems	Capable of generating constant and more reliable cyber-physical interaction for real-time problem	Not disclosed	This paper does not consider distribution of works to nodes to scale the resources
5.	Sood and Mahajan [44]	Used temporary network analysis and J48 decision tree to monitor MBDs	Control of outbreak of mosquito-borne diseases (MBD) at infant stage	Cyber-physical system	High-performance classification accuracy and low rate of differentiating MBDs	Not disclosed	The proposed technique lacks the ability to quarantine the detected MBD_s
6.	Yaseen et al. [54]	Real-time monitoring and detection of collision attack in IoT	Data retrieval and detection of all types of attack	Data aggregation using averaging algorithms	Tracking of malicious node from one point to another in IoT environment	Not disclosed	The model lack authentication system to reduce collusion intruder

Table 6 Analysis of computational/evolutionary intelligence techniques

S. no.	References	Proposed technique	Problem addressed	Comparison method	Major findings	Parameter used	Limitation
1.	Sun et al. [47]	Evolutionary game using credible third party	Reduction in attack behaviour	Not stated	Increase in user's benefit and maintenance of security mechanism	Not disclosed	The authors did not specify the behavioral pattern
2.	Neto et al. [34]	Fog-FISVER (framework for intelligent public safety in vehicular environment)	Efficient and cost less crime detection	FISVER (framework for intelligent public safety in vehicular environment)	Better performance with higher efficiency	Not disclosed	Timely notification on rate of crime detection on mobile application is not investigated
3.	Sood and Mahajan [44]	J48 decision tree to monitor MBDs	Control of outbreak of mosquito-borne diseases (MBD) at infant stage	Cyber-physical system	High-performance classification accuracy and low rate of differentiating MBDs	Not disclosed	The proposed technique lacks the ability to quarantine the detected MBD$_s$

connected and the developed prototype influenced analysis of geospatial-health data. The combined techniques of mist and fog devices have the advantage of reducing the storage requirement, transmission power, and reduced latency which holistically increase performance efficiently. The experimental result shows that overlay analysis is a viable method for geospatial-health data visualization. The authors used Malaria vector-borne diseases positive maps of Maharashtra in India to perform overlay analysis. Nevertheless, the proposed techniques are not subjected to other Big data analysis to determine it robustness and efficient.

Santoro et al. [39] showcase foggy, which is an architecture framework and a system platform that depend on open-source technology. The architectural workload arrangement and application workload negotiate resources and give support to IoT operation for multi-tier, distributed, heterogeneous, and decentralized cloud platform. The team asserts that foggy is expected to give support to 5G network and IoTs and also make available a platform for infrastructure and tenant to offer negotiation, scheduling, and workload. The authors recommend pricing and billing to be incorporated to tackle the infrastructure and tenant owners as future work. However, the team did not put load balancing in the workload arrangement into consideration.

Service broker policy for fog-computing environment which enables users to select optimal datacenters to satisfy their requests based on the security strength of the datacenters with respect to cost and response time within them was initiated. The new proposed scheme provides internal mechanism that can adjust and adapt to changes in the datacenter dynamically as opposed to the existing scheme [3]. The result of the experimental setup proved that the proposed scheme perform well than the existing approach. Nonetheless, evaluation of the security strength of the IoT devices is needed using ideal trust model to prove the security strength of the datacenter.

Guan et al. [13] critically analyzed and discussed design issues associate with data security and privacy in fog computing. The authors came up with different security and privacy design challenges in the fog layer and conclude that techniques applied to resolve data-security problem in the cloud computing cannot be applied directly in fog-computing platform to solve data-security issues. The team emphasized that auditable method of securing cloud data storage is not applicable in fog computing, because the data that are meant to be audited are never the real data from end user; rather, it is the processed data from the fog nodes. Furthermore, this paper pointed out that integrity, verification, minimum overhead, public auditing, support dynamics, and access efficiency, authorization revocation, and fine-grain access control are the preferred auditable data storage properties that are needed in fog computing. However, the researchers did not examine and compare the security of the fog devices with the cloud security.

An architecture that supports fog computing that can be installing in any service that is combined with SDNs to improve the network resilience [31]. The framework was tested through IP spoofing security application which proved the viability of the platform through series of experiment conducted. Addition of traffic management and machine-learning-based intrusion detection are to be considered as future work. Nevertheless, the new framework is not dynamic enough to handle network resilience in other platform.

Neto et al. [33] proposed a multi-tenant load distribution algorithm in fog computing that is named MtLDF. The researcher's sole aim of developing MtLDF is to consider delay and priority requirement to burst the load balancing in fog environment. The result from the experimental setup proved that MtLDF is capable of distributing the load in an effective and more efficient way as compared with delay-driven load distribution (DDLD). The team intends to improve the load balancing through the fog–cloud layers with respect to disk input/output operations as future work. However, the distribution technique is only effective in fog-computing environment.

Li [23] investigated security issues by incorporating fog computing into internet of energy IOE. The new scheme (FSDR) was designed to avoid collusion attacks through access-control encryption techniques. Through mathematical model, the researchers were able to discover the collusion attack and the possible defense method. Evaluation of the scheme was conducted through an algorithm and improvement on energy utilization. Nevertheless, while the new scheme is said to be efficient, more evaluation is need to prove the system's scalability in other IoE cases. Mahmud et al. [28] designed an interoperable fog base IoT-healthcare solution framework that is integrated with cloud–fog services to move the cloud-based system to a new level, where health care solution is incorporated. The result of the simulated experiment shows latency reduction, improvement on data communication, and relatively low power consumption. However, the authors did not investigate the impact of the proposed techniques on CPU utilization and sensors increase on the application demand. Bedi et al. [5] proposed an efficient and secure multi-cloud storage approach for mobile devices MWC for free storage capacity, energy consumption, data usage, and sensitivity of data security. The team also embedded security system that caters for data security which present distribution of login credential of users. Similarly, data-splitting mechanism is implemented to divide data into part and stored on different CSPs, such that access granted to unauthorized persons will be counterproductive. The result indicates the efficiency of battery, CPU, and other data device utilization. Conversely, the researchers did not experiment with video data to determine the CPU and memory utilization of the new system.

Programming architecture scheme that allows for share computing on fog-to-cloud environments [26]. The framework execute applications in a distributed manner of computing which include cloud resources and fog devices such as mobile phones, cloudlets and small-cloud. The scheme significantly improved on new distributed data management system that allows efficient and effective sharing of information of data on different platforms. The tested result gives clear view of run time refactoring and extension that does not have damaging effect to the performance of the execution when the tasks are offloaded from close nodes. Nevertheless, more optimization needed to be conducted to check the mechanism of the security in the scheduling policy.

Rahmani et al. [36] take advantage of gateways at the network's edge to provide powerful services which include local storage, real-time local data processing, and embedded data mining. The authors proposed fog-computing architecture in healthcare IoT system that can consist of a geo-distributed intermediary layer of intelligence that exists between the sensor nodes and the cloud. The team also developed a monitoring system smart e-health gateway named UT gate that is capable of handling some health issues. Early warning score (EWS) was also integrated and implemented by the researchers for health-monitoring system that can support energy efficiency, system intelligence, interoperability, high performance, security, and reliability. Nonetheless, the underlying sensor sensitivity needs to be investigated to ensure the performance and reliability of the monitoring system.

Rios et al. [37] observed that certain security mechanism needs to be put in place to fully derive the benefit of fog computing. This is necessary to prevent the setback the conceived benefit will suffer, due to the various security bridge activities by attackers. The authors pointed out that the previous effort about security solution only protected the fog nodes without due consideration to the environment and the interaction between the fog and the ecosystem. The researchers came up with the development of SMOG–CORE for tackling security services for the infrastructure and SMOG–Dev service to enable protective interaction between the end users and the infrastructure. This paper highlighted the main security threats and attacks that might affect the infrastructure at the nodes (edges) and invariably extend the impact of the attack to the immediate environment. Denial of service, data leakage, manipulation, and impersonation are the possible security threats. The basic security services suggested by the authors for enabling federated and to protect fog infrastructure includes service interconnect of fog elements, authentication and authorization, protection of virtualized environment, and situation awareness mechanisms. Other security service that supports the cooperation and secure interactions with one another is: trust service, distributed decision making, private support, and digital evidence management. However, the study could not come up with clear digit evidence and, therefore, suggested further security research in the area of fog computing.

Lee et al. [22] explained that the gateways serving as fog devices may be compromise by man-in-the-middle attack. In their presentation, the team observed that it is difficult to use encryption and decryption algorithm to secure communication between the fog devices and IoT devices. This is because the formal and the later consume large amount of battery on mobile devices. The authors pointed out that fog computing that is based on IoT devices is limited in computing and resources. As a result, it becomes difficult to detect the root kit and the various types of malicious code that is present in the fog nodes. The team combined a fog node and the cloud to visualize a fog-computing paradigm that produces high quality of services to the users to make up for the lapses of cloud in internet-of-things environment. More so, the authors analyzed man-in-the-middle attack, intrusion detention, malicious detention techniques in fog environments, malicious fog nodes problem, data protection, and data management as the major security challenges and privacy issues militating against fog-computing model. While the researchers recommended a future direction that will develop a system to collect and analyze the generated log from fog computing, which will provide vital information to the user, this paper failed to developed a model that could serve as preventive measures and solution to the problems analyzed.

Wireless technology was viewed by Kumar et al. [21] as the main factor responsible for insecurity of the internet. Sniffing, spoofing, jamming, etc., are said to be the various attacks that could have significant effect on fog computing between the fog nodes and the centralized devices. The authors proposed prevention of location and data privacy security through the use of identity obstruction techniques. They achieved this by making fake node at various fog connections in conjunction with fake document to make it look legitimate and thereby implicitly make the unauthorized user to download fake document. They also use the unauthorized user's system to locate the Mac address of the system and eventually send the content to the regional cloud to block more request and to be able to evaluate the location of the authorize user. Nonetheless, the researchers were unable to achieved optimum security and, therefore, suggested the integration of only one fake fog node, such that it will automatically replicate itself to make it more complex for location identification.

Ni et al. [35] highlighted forgery, spam, Sybil, jamming, eavesdropping, denial of service, impersonation, collusion, and man-in-the-middle as the possible attack that could be launch to disrupt the fog computing. The study further identified authentication, access control, lightweight protocols design, and trust management as viable techniques to overcome security challenges. However, despite the security challenges and the suggested solution by the authors, the solutions are not without its own disadvantages. The researchers, therefore, recommended the building of block chain between the cloud and IoT devices, to strengthen the fog-computing architecture to become more trusted, reliable, and even more powerful.

Mart [30] proposed virtual medical devices to protect and secure medical cyber-physical system due to the obvious challenges that existed in the existing system. The team came up with a framework that could support the mobile edge and fog architecture that is capable of using NFL and SDN techniques to enable real-time management of the former system. The designed framework defines some management policy that is meant to use virtualization techniques (VNF) and software define–define networking applications as well as medical in conjunction with the patient's location, important signs, medical devices, and communication of the networks. The result of the new system shows efficiency, low latency, flexibility, and the capability of detecting and mitigating attacks in a timely manner. However, the team does not subject the new system to several kinds of attacks to ascertain the efficiency of the security scheme.

Wang et al. [50] developed three-layer fog-based architecture that can upload data from wireless sensor networks (WSNs) to the cloud. The proposed framework is segmented to include the sing layer, fog layer, and routing layer. The researchers used DCF algorithm to maximize and minimize the latency of the system. The result of the proposed technique shows improvement by reducing transmission delay by 45% and also conserves energy consumption when compared to unscheduled scheme. However, more evaluation of the method is needed to ascertain the latency efficiency of the architecture.

Stojmenovic et al. [46] introduced a stand-alone authentication mechanism to realize user authentication when there is no established connection to the cloud server. This was achieved through hybrid encryption and attribute-based encryption. The former is a procedure to share data with a particular party in encryption, while the latter is information such as smart grid. Extending hybrid encryption into one-to-many setting can address the connection issue if the two fog devices are in different areas. This authentication method enables users to be authenticated and has permission to establish connection between the fragile cloud and the fog devices. The team pointed out that this approach creates another problem of calculating increase in smart users' card, especially if a new equipped device that is to act as stand-alone is added. This problem according to the authors can be subdued through cryptographically primitive-attribute-based encryption method. The authors described the attribute-based encryption as a viable tool, for providing data without necessarily having the fore knowledge of the receiver of the data. This provides flexible sharing of data in flexible way more than the usual end-to-end encryption. However, the proposed technique is not capable of authenticating and authorizing users in a distributed manner. Table 7 presents the analysis of the problems and the major research findings on security challenges in "other category" of fog computing.

5 Data set analysis

This section presents analysis of the data sets with the URL addresses and the number of instances that were applied. This is intended to inform the researchers about the various applicable data sets that were used in the study, as shown in Table 8.

6 Discussion

This section discusses the various techniques, with most popular security protection and the taxonomy created, based on the security techniques found in the fog-computing-related literatures. The trend of publication and the future trend of publication are also discussed. Decoy technique is quite effective in addressing authentication and account hijacking, Markov's model is effective in detecting malicious edge devices in fog-computing environment, block chain technique addresses authentication problem and also reduces delay time, while denial of service is best handled by situational awareness mechanism combined with trust management services.

The created taxonomy in Fig. 5 classified the various security techniques into machine-learning technique, cryptographic technique, computational/evolutional intelligence, and other techniques. The classification of these techniques in this study differentiates this paper from the existing review on fog computing.

The trend of publication with respect to the authors, the range of time, and the most recent publications is presented in Fig. 3. Table 5 contains seven columns which show the analysis of the problems and the major research findings. It consists of the column for the problem addressed, the research major findings, the parameters used, and the limitations of the various techniques. However, data set availability constitutes a major challenge in this research due to the fact that most of the authors did not disclosed the data set or parameters used for the research. The tables clearly indicated that most of the techniques could not address all threats noticeable in fog platform. Some security problems were partially addressed, while others were constrained due to the limitations of the proposed techniques. However, from the survey and the research analyses, man-in-the-middle attack investigation remains a top priority for the future.

7 Unresolved challenges and future research work

This section points out the unresolved challenges in fog-computing model and future research direction.

The fog computing is an emerging area of interest to the researchers. Serious research works are ongoing to unravel the benefit of the model [13]. There are some unresolved security problems and challenges faced by this computing model.

1. Man-in the-middle attack: MITM remains a problem that is yet to be resolved in fog-computing environment. Fog devices within the environment are usually out of surveillance, such that attackers can easily reply the communication. Encryption and decryption method is not suitable to counter the MITM attacks because of high consumption of battery power especially in mobile phones that use 3G [7]. Though the previous research shows that it consumes small amount of network resources, the threats very are difficult to be address.
2. Denial of service (DOS) and distributed denial of service (DDOS): DDOS is a type of network attack that blocks the legitimate users to have access to fog or cloud resources. Intrusion detection is the usual recommended method for resolving the problem. However, in fog environment, there is no known solution available that can handle DDOS issues effectively at present.
3. Identity authentication: there are many authentication schemes that have been developed for internet services, e.g., (fingerprint, face recognition, and iris recognition). IoT devices mobility is a necessary factor to be considered, because user of fog computing may move from one coverage area to another. Each of the nodes authenticates the users when accessing services. However, when the users increase in number, the latency may not be supported in real time. Even though cooperative authentication schemes are used to reduce authentication overhead, it is necessary to design and implement an authentication scheme that support Fog nodes to confirm user's identification before offering services.

Furthermore, the investigation of MITM attack between the fog nodes and the cloud, and vice versa using swarm-intelligence optimization techniques on the platform of iFog simulator to determine the stealthy nature of the attack is recommended as future research direction.

Table 7 Analysis of other techniques

S. no.	References	Proposed technique	Problem addressed	Comparison method	Major findings	Parameter used	Limitation
1.	Rios et al. [37]	Deployment of situational awareness mechanisms techniques in conjunction with trust management services	The security protection mechanism addressed the threat of denial of service, data leakage, manipulation and impersonation	Situation awareness mechanisms	Advanced security such as trust management services is said to be essential to unknown entity interacting with fog	Not disclosed	The security mechanism does not put all other security threat associated with fog and cloud into consideration
2.	Lisbon and Kavitha [24]	Decoy techniques and parametric based authentication method	Authentication And account hijacking	Not stated	The model provide authentication to user which addressed data breach or combination of both for account hijacking	Not disclosed	The techniques is not capable to address other security threats in fog computing
3.	Stojmenovic and Wen [45]	Hook technique	The techniques addressed the stealthy nature of man-in-the-middle attack	Encryption and decryption methods	It exposed the negligible consumption of video communication and concluded that man-in-the-middle attack is simple to launch but difficult to addressed	Processor usage (cpu) and memory utilization I/O rate	The technique is not capable of exposing the major impact of man-in-the-middle attack
4.	Lee et al. [22]	Hybridization of fog nodes, cloud and sensor to explore IoT fog	Configuration of the secure fog-computing environment through security technology	Cloud IoT	Dynamic analysis techniques is required to monitor fog nod in real time	Not disclosed	The method is unable to collect and analyze various logs that were generated in fog-computing environment
5.	Kumar et al. [21]	Decoy techniques in combination with theoretical method for data location privacy	The proposed techniques used theoretical method to address common security threats	Note stated	Location and data privacy prevention through the use of MAC address to block fake node request to determine the location of the fake node	Not disclosed	The proposed theoretical technique is not robust enough to address all security threat in fog-computing environment
6.	Shrophire [42]	Integration of cloud–fog platform to support a wide variety of optimized services	The techniques addressed vulnerabilities in confidentiality, integrity and availability	Not stated	Distributed image vulnerability prevention and the integration of asymmetric techniques for verifying node identities to prevent weak authentication	Not disclosed	The novel platform can only address security vulnerability within the edge devices but not dynamic enough to address security threats from fog to cloud and vice versa
7.	Wang et al. [51]	Decoy techniques in combination with user behaviour profiling	Detection of illegitimate access to information	Game theoretic energy schedule (GTES)	The combine techniques recognizes and monitor legitimate or masqueraders	Not disclosed	Not dynamic enough to minimize other attack on fog computing

Table 7 (continued)

S. no.	References	Proposed technique	Problem addressed	Comparison method	Major findings	Parameter used	Limitation
8.	Ni et al. [35]	Block chain techniques	The techniques addressees authentication problem in multiple fog nodes	Core-based cloud-computing infrastructure	The implementation of the proposed techniques will make a secure, reliable and trustworthy fog node	Not disclosed	The block chain management is not capable of handling overhead on a single fog node due to the restricted storage resources
9.	Zahra et al. [56]	Intrusion detection technique in combination with Hellman key exchange	Man-in-the-middle attack (MITM)	Not state	Attack does not cause significant change in Memory and CPU consumption of fog node	Processor usage (cpu) and memory utilization I/O rate	Suggested security solutions are insufficient enough to protect the fog platform against CIA
10.	Rios et al. [37]	Holistic analysis of edge paradigm	Security threats, challenges and inherent mechanism in edges paradigm	Not stated	The authors find out that most research does not follow interdisciplinary approach rather studies only focus particular edge paradigm	Not stated	This paper failed to evaluate the impact that denial of service attack, rogue data centre may have on the service infrastructure
11.	Mahmud et al. [28]	Interoperable fog-based IoT-healthcare solution framework	Incorporation of healthcare solution into cloud-based system	General cloud-based IoT-healthcare solution	Latency reduction, low power consumption	Not stated	No experiment conducted on CPU utilization and increase on application demand
12.	Kang et al. [17]	Fog-computing supported IoV called (F-IoV)	Location privacy challenges of IoV	Cloud-assisted IoV	Secure communication, privacy preservation for vehicle	Not disclosed	The proposed scheme cannot address sparse vehicles
13.	Fu et al. [12]	Retrieval tree and index encryption techniques with KNN algorithm	Privacy-preserving data search	Not stated	Improved storage data security and retrieval in IIoT	Not disclosed	The new scheme is not robust enough to handle multiple retrieval
14.	Liu et al. [25]	Hybrid privacy-preserving clinical decision support system (HPCS)	Monitoring and predicting diseases for patient health status	Neural networks (NNs)	Ease of monitoring of patient health status that enable patient to query the sever and get timely response from fog or cloud	Not stated	The techniques lack ability to influence better decision
15.	Wang et al. [49]	Data aggregation and data filter	Resolves the issues of too large data communication over vehicular application	Not stated	Security forensic challenges solutions	Not stated	The scheme is not robust to address all security threats
16.	Neto et al. [33]	Multi-tenant load distribution algorithm	Delay and priority requirement	Delay-driven load distribution (DDLD)	Load distributing efficiency	Not disclosed	The distribution scheme is only effective in fog computing

Table 7 (continued)

S. no.	References	Proposed technique	Problem addressed	Comparison method	Major findings	Parameter used	Limitation
17.	Rahmani et al. [36]	Monitoring smart e-health gateway (UT-gate)	Real-time local data processing, local storage and embedded data mining	Smart e-health gateway	Energy efficiency support, high-performance, security reliability	Not disclosed	The sensor sensitivity is not dynamic to ensure medical data privacy of patients
18.	Koo and Hur [20]	Secured data deduplication scheme	Consistency in privacy through user-level public key and cipher text	Secure data deduplication using fixed shared key	Reduction of communication level and number of keys without security degradation	Not disclosed	The new technique is highly dependent on user-level public keys update
19.	El-Latif et al. [10]	Quantum steganography	Securing of flow of messages in fog and cloud IoT	Quantum information processing (QIP)	Secured architecture against visible attack	Not stated	Memory utilization and CPU consumption is not investigated
20.	Singh et al. [43]	Markov model and virtual honeypot	Detection of malicious edge devices in fog environment	Honeypot	Maintenance of log repository and defend it from unknown attack	Not stated	The authors did not investigate wider ethical hacking activities
21.	Mukherjee et al. [32]	End-to-end cloud–fog security middleware using pre-share keys (PSK)	Network security located at the user fog	Core cloud network using system level or application	Fast track secure communication	Not stated	More investigation is needed to confirm the extent of the security control
22.	Donovan et al. [8]	Real-time embedded machine-learning application	Data protection security and privacy	Industrial cyber-physical systems	Capable of generating constant and more reliable cyber-physical interaction for real-time problem	Not disclosed	This paper does not consider distribution of works to nodes to scale the resources
23.	Santoro et al. [39]	Open-source technologies	Resource negotiation, scheduling and workload	Workload management	Architecture Support to 5G network and IoTs	Not disclosed	This paper does not address security associating with the new scheme
24.	Wang et al. [49]	Three-layer fog-based framework in conjunction with DCF algorithm	To upload data wireless sensor networks to the cloud and to minimize and maximize latency of system	Unscheduled scheme (US)	Reduced transmission delay and conserved energy consumption	Not disclosed	The scheme not tested with rate of CPU consumption
25.	Sharma et al. [40]	Blockchain-based distributed cloud framework	Reduce delay time, real-time attack detention	Core-based cloud-computing infrastructure	Secure and improved response time and on-demand access with low-cost	Not stated	More investigation is needed with respect to memory utilization of the scheme

Table 7 (continued)

S. no.	References	Proposed technique	Problem addressed	Comparison method	Major findings	Parameter used	Limitation
26.	Yang et al. [53]	Secure positioning with one dimension and three dimension protocol	Protection of location privacy	Signal strength measurement	Two dimension support region of any interval between two protocol, while tree dimension support only region shapes	Not stated	The author does not highlight the types of security attack the framework can control
27.	Yang et al. [53]	Bounded retrieval model	Secure positioning protocol with location privacy	Signal strength measurement	Secured and less access time to search the encrypted data	Not disclosed	The scheme lack capability to address all kinds of attacks
28.	Lordan et al. [26]	Virtualization technique and software define networking	Share computing on fog-to-cloud environment	COMPSs programming framework	Effective and efficient sharing of information of data on different platforms	Not disclosed	The novel scheme is not exposed to intensive evaluation to justify the efficiency
29.	Bedi et al. [5]	Multi-cloud storage approach	Energy consumption, data usage, storage capacity and sensitivity of data security	Multi- cloud storage systems (MCSS)	CPU and battery efficiency and devices utilization	Not disclosed	No experiment to determine the CPU and memory utilization
30.	Wang et al. [48, 50]	Fog-based cloud storage scheme	Preventing user data from impending cyber attack and securing data privacy	Encryption technique	Faster transmission rate between the fog server environment than cloud server environment	Not disclosed	The scheme is not investigated with man-in-the-middle attack
31	Abbasi and Shah [2]	Modification of decoy method	Classification of fog architecture into three tiers to address security challenges	Lightweight cryptography	Authentication and authorization is found to be the best security techniques	Not disclosed	This paper does not consider other attacks which could maliciously hinder the data security
32.	Yaseen et al. [54]	Real-time monitoring and detection of collision attack in IoT	Data retrieval and detection of all types of attack	Data aggregation using averaging algorithms	Tracking of malicious node from one point to another in IoT environment	Not disclosed	The model lack authentication system to reduce collusion intruder
33.	Zahra et al. [56]	Shibboleth protocol	Data and security access management	Digital signatures	Better security mechanism	Not state	The authors did not highlight the types of security threat that is best controlled by Shibboleth scheme
34.	Jiang et al. [16]	CP-ABE in conjunction with KP-ABE	Protection of key-delegation abuse	CP-ABE	More efficient in attribute arrangement	Not stated	No established investigation to determine the level of support of the scheme for other access structure

Table 7 (continued)

S. no.	References	Proposed technique	Problem addressed	Comparison method	Major findings	Parameter used	Limitation
35.	Arya and Dave [3]	Security-based service broker policy (SbSBP)	Selection of optimal data centres	DSBP (dynamic service broker policy)	Better performance with internal mechanism adjustment	Not stated	The experimental evaluation is not based on trust model
36.	Guan et al. [13]	Data security and policy	Auditable method of securing cloud and fog data	Not stated	Auditable method not applicable in fog-computing platform	Not stated	More investigation is needed to verify the assertion
37.	Modarresi et al. [31]	Network resilience framework	Network application and communication control	A multipath load balancer	Timely detection and mitigation of attacks	Not stated	The scheme is not subjected to several kinds of attack to prove it efficiency
38.	Zhang et al. [57]	Decisional bilinear Diffie–Hellman	Removal of encryption and decryption bottleneck	CP-ABE	Secure scheme and less cost of computation	Not disclosed	This paper did not highlight the security type that is control by the scheme
39.	Sun et al. [47]	Evolutionary game using credible third party	Reduction in attack behaviour	Not stated	Increase in user's benefit and maintenance of security mechanism	Not disclosed	The authors did not specify the behavioral pattern
40.	Barik et al. [4]	Win–win spiral model	Storage requirement reduction, transmission power and reduced latency	Cloud-based framework	Overlay analysis is a better method for geospatial-health data visualization	Not disclosed	The Scheme is not subjected to big data analysis
41.	Wang et al. [48, 50]	Anonymous and secure aggregation scheme	Bandwidth and time conservation	Pseudonyms technique	Highly efficient and secure model	Not disclosed	The security notion cannot dynamically address all attack threats
42.	Neto et al. [34]	Fog-FISVER Framework for Intelligent Public Safety in Vehicular Environment	Efficient and cost less crime detection	FISVER (framework for intelligent public safety in vehicular environment)	Better performance with higher efficiency	Not disclosed	Timely notification on rate of crime detection on mobile application is not investigated
43.	Li [23]	FSDR through access control and encryption	Collusion attack and defense methods	Centralized and decentralized scheme	Improved energy utilization and efficiency	Not disclosed	More evaluation is needed to determine the system's scalability in IoE cases
44.	Huang et al. [15]	Forensics techniques	Reduction of road traffic congestion and car accidents	Not stated	Real-time identification, collection, and analysis of data	Not Stated	forensic requirement presented cannot address all available security threats
45.	Xiong et al. [52]	AES and SSL	Prevention of unauthorized access to information	Cryptographic parameters	Secure and effective way to prevent attacker to access unauthorized information	The average time required for the security level and the search for data	The combined security parameters cannot address man-in-the-middle attack

Table 7 (continued)

S. no.	References	Proposed technique	Problem addressed	Comparison method	Major findings	Parameter used	Limitation
46	Mart [30]	VNF and SDN	Network control and patient's location	Virtual medical device (VMD)	Capability of detecting and militating against attacks in a timely manner	Not stated	The new scheme not exposed to all different types of attack to justify the claim of the security scheme
47.	Ebebe and Naveen [9]	Deep-learning algorithm (DL)	Cyber-attack detection	Shallow algorithms	Improvement on the accuracy and efficiency of cyber-attack detection	NSL–KDD data set	The authors did not verify the scheme using different data sets
48.	Escamilla-Ambrosio et al. [11]	Not stated	Optimizing resources, bandwidth usage and best fit approaches	Not stated	Networking and storage capabilities	Not stated	The experiment lacks proper evaluation to justify the claim

Table 8 Data set analysis

S. no.	References	Data set	URL address	No. of instances
1.	Liu et al. [25]	UCI machine-learning repository (breast cancer Wisconsin)	Note stated	699
2.	Singh et al. [43]	Pytbull	Note stated	80
3.	Barik et al. [4]	Quantum GIS	Note stated	None
4.	Donovan et al. [8]	PMML-encoded machine-learning model	Note stated	1000
5.	Ebebe and Naveen [9]	NSL–KDD data set	Note stated	150

8 Conclusion

This paper presents a systematic review on security challenges in fog computing. This review discussed and summarized the various techniques applied to solve the security problems within the fog-computing environment and their limitations. This study reveals that most of the security techniques that were applied by various researchers are not dynamic enough to completely address all the fog security problems. In addition, it was found that most research does not follow interdisciplinary approach to arrive at major findings. Rather, studies were focused on particular paradigm. MITM attack, DOS, and identity authentication constitute major challenges that needed researchers' attention. Further research path is directed to deployment of swarm-intelligence optimization techniques to address MITM attack within the fog-computing environment.

References

1. Abdulhamid SM, Latiff MS (2017) A checkpointed league championship algorithm-based cloud scheduling scheme with secure fault tolerance responsiveness. Appl Soft Comput 61:670–680
2. Abbasi BZ, Shah MA (2017) Robust practices. In: Proceedings of the 23rd international conference on automation & computing, University of Hudders Field, Hudders Field, UK, 7–8 September 2017, pp 7–8
3. Arya D, Dave M (2017) Security-based service broker policy for fog computing environment. In: IEEE 8th ICCCNT 2017, Department of Computer Engineering
4. Barik RK, Dubey AC, Tripathi A, Pratik T, Lenka K, Pratik T et al (2018) Mist data: leveraging mist computing for secure and scalable architecture for smart and connected health. Procedia Comput Sci 125:647–653. https://doi.org/10.1016/j.procs.2017.12.083
5. Bedi RK, Singh J, Gupta SK (2018) MWC: an efficient and secure multi-cloud storage approach to leverage augmentation of

multi-cloud storage services on mobile devices using fog computing. J Supercomput. https://doi.org/10.1007/s11227-018-2304-y
6. Bilal K, Khalid O, Erbad A, Khan SU (2018) Potentials, trends, and prospects in edge technologies: fog, cloudlet, mobile edge, and micro data centers. Comput Netw 130:94–120. https://doi.org/10.1016/j.comnet.2017.10.002
7. Christopher HA, Yakubu J, Mohammed AD (2018) An architectural framework for ant lion optimization-based feature selection technique for cloud intrusion detection system using bayesian classifier. imanagers J Cloud Comput 5(2):36
8. Donovan PO, Gallagher C, Bruton K, Sullivan DTJO (2018) A fog computing industrial cyber-physical system for embedded low-latency machine learning industry 4.0 applications. Manuf Lett. https://doi.org/10.1016/j.mfglet.2018.01.005
9. Ebebe A, Naveen C (2018) Deep learning: the frontier for distributed attack detection in fog-to-things computing. IEEE Commun Mag 56:169–175. https://doi.org/10.1109/MCOM.2018.1700332
10. El-Latif AAA, Abd-El-Atty B, Hossain MS, Member S (2018) Secure quantum steganography protocol for fog cloud internet of things. IEEE Spec Sect Recent Adv Cloud Radio Access Netw 6:10332–10340. https://doi.org/10.1109/ACCESS.2018.2799879
11. Escamilla-Ambrosio PJ, Rodríguez-Mota A, Aguirre-Anaya E, Acosta-Bermejo R, Salinas-Rosales M (2018) Distributing computing in the internet of things : cloud, fog and edge computing overview, pp 87–115. https://doi.org/10.1007/978-3-319-64063-1_4
12. Fu J, Liu Y, Chao H, Member S, Bhargava BK (2018) Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing. IEEE Trans Ind Inform. https://doi.org/10.1109/TII.2018.2793350
13. Guan Y, Shao J, Wei G, Xie M (2018) Data security and privacy in fog computing. IEEE Netw. https://doi.org/10.1109/MNET.2018.1700250
14. Hu P, Dhelim S, Ning H, Qiu T (2017) Survey on fog computing: architecture, key technologies, applications and open issues. J Netw Comput Appl 98:27–42. https://doi.org/10.1016/j.jnca.2017.09.002
15. Huang C, Lu R, Choo KR (2017) Vehicular fog computing: architecture, use case, and security and forensic challenges. IEEE Commun Mag 55:105–111. https://doi.org/10.1109/MCOM.2017.1700322
16. Jiang Y, Susilo W, Mu Y, Guo F (2018) Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing. Future Gener Comput Syst 78:720–729. https://doi.org/10.1016/j.future.2017.01.026
17. Kang J, Yu R, Huang X, Zhang Y, Member S (2017) Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles. IEEE Trans Intell Transp Syst. https://doi.org/10.1109/TITS.2017.2764095
18. Khan S, Parkinson S, Qin Y (2017) Fog computing security: a review of current applications and security solutions. J Cloud Comput 1:1. https://doi.org/10.1186/s13677-017-0090-3
19. Kitchenham B, Brereton OP, Budgen D, Turner M, Bailey J, Linkman S (2009) Systematic literature reviews in software engineering—a systematic literature review. Inform Softw Technol 51(1):7–15
20. Koo D, Hur J (2018) Privacy-preserving deduplication of encrypted data with dynamic ownership management in fog computing. Future Gener Comput Syst 78:739–752. https://doi.org/10.1016/j.future.2017.01.024
21. Kumar P, Zaidi N, Choudhury T (2017) Fog computing: common security issues and proposed countermeasures. In: Proceedings of the 5th international conference on system modeling and advancement in research trends, SMART 2016, pp 311–315. https://doi.org/10.1109/SYSMART.2016.7894541
22. Lee K, Kim D, Ha D, Rajput U, Oh H (2015) On security and privacy issues of fog computing supported Internet of Things environment. In: 2015 International conference on the network of the future, NOF 2015. https://doi.org/10.1109/NOF.2015.7333287
23. Li G (2018) Fog computing-enabled secure demand response for internet of energy against collusion attacks using consensus and ACE. IEEE Spec Sect Internet Energy Archit Cyber Secur Appl 6:11278–11288. https://doi.org/10.1109/ACCESS.2018.2799543
24. Lisbon AA, Kavitha R (2017) A study on cloud and fog computing security issues and solutions. Int J Innov Res Adv Eng 3(4):2349–2163. http://ijirae.com/volumes/Vol4/iss03/03.MRAE10083.pdf
25. Liu X, Deng RH, Yang Y, Tran HN, Zhong S (2018) Hybrid privacy-preserving clinical decision support system in fog–cloud computing. Future Gener Comput Syst 78:825–837. https://doi.org/10.1016/j.future.2017.03.018
26. Lordan F, Lezzi D, Ejarque J, Badia RM (2018) An architecture for programming distributed applications on fog to cloud systems, 2. In: Heras DB, Bougé L (eds) Euro-Par 2017 workshops, vol 10659. LNCS. Springer International Publishing AG, Berlin, pp 325–337
27. Madni SHH, Latiff MSA, Ali J (2019) Multi-objective-oriented cuckoo search optimization-based resource scheduling algorithm for clouds. Arab J Sci Eng 44(4):3585–3602
28. Mahmud R, Koch FL, Buyya R (2018) Cloud–fog interoperability in IoT-enabled healthcare solutions. In: ICDCN'18: 19th international conference on distributed computing and networking, January 4–7, 2018, Varanasi, India. ACM, New York, NY, USA, pp 4–7. https://doi.org/10.1145/3154273.3154347
29. Mahmud R, Kotagiri R, Buyya R (2018) Fog computing : a taxonomy, survey and future directions. In: Di Martino B et al (eds) Internet of everything, internet of things. Springer Nature, Singapore. https://doi.org/10.1007/978-981-10-5861-5_5
30. Mart G (2018) Sustainable securing of medical cyber-physical systems for the healthcare of the future. Sustain Comput Inform Syst. https://doi.org/10.1016/j.suscom.2018.02.010
31. Modarresi A, Gangadhar S, Sterbenz JP (2017) A framework for improving network resilience using SDN and fog nodes. In: 2017 9th international workshop on resilient networks design and modeling (RNDM). https://doi.org/10.1109/RNDM.2017.8093036
32. Mukherjee B, Wang S, Lu W, Neupane RL, Dunn D, Ren Y et al (2018) Flexible IoT security middleware for end-to-end cloud–fog communication. Future Gener Comput Syst. https://doi.org/10.1016/j.future.2017.12.031
33. Neto ECP, Callou G, Aires F (2017) An algorithm to optimise the load distribution of fog environments. In: 2017 IEEE international conference on systems, man, and cybernetics (SMC), Banff Center, Banff, Canada, October 5–8, 2017, (October), pp 1292–1297
34. Neto AJV, Zhao Z, Rodrigues JJPC, Member S, Camboim HB, Braun T (2018) Fog-based crime-assistance in smart IoT transportation system. IEEE Access 6:11101–11111
35. Ni J, Zhang K, Lin X, Shen X (2017) Securing fog computing for internet of things applications: challenges and solutions. IEEE Commun Surv Tutor 20:601–628. https://doi.org/10.1109/COMST.2017.2762345
36. Rahmani AM, Nguyen T, Negash B, Anzanpour A (2018) Exploiting smart e-health gateways at the edge of healthcare internet-of-things: a fog computing approach. Future Gener Comput Syst 78:641–658. https://doi.org/10.1016/j.future.2017.02.014
37. Rios R, Roman R, Onieva JA, Lopez J (2017) From SMOG to fog: a security perspective. In: 2017 2nd International conference on fog and mobile edge computing, FMEC 2017, pp 56–61. https://doi.org/10.1109/FMEC.2017.7946408

38. Roman R, Lopez J, Mambo M (2018) Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges. Future Gener Comput Syst 78:680–698. https://doi.org/10.1016/j.future.2016.11.009
39. Santoro D, Zozin D, Pizzolli D, De Pellegrini F, Cretti S Createnet FBK, Cascata D (2017). Foggy : a platform for workload orchestration in a fog computing environment. In: 2017 IEEE 9th international conference on cloud computing technology and science, pp 9–12. https://doi.org/10.1109/CloudCom.2017.62
40. Sharma PK, Chen M, Park JH (2018) A software defined fog node based distributed blockchain cloud architecture for IoT. IEEE Spec Sect Intell Syst Internet Things 6:115–124. https://doi.org/10.1109/ACCESS.2017.2757955
41. Shirazi SN, Gouglidis A, Farshad A, Hutchison D (2017) The extended cloud: review and analysis of mobile edge computing and fog from a security and resilience perspective. IEEE J Select Areas Commun 35(11):2586–2595
42. Shropshire J (2014) Extending the cloud with fog : security challenges & opportunities. In: Americas conference on information systems, pp 1–10
43. Singh A, Sandhu R, Sood SK (2018) A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Comput Secur 74:340–354. https://doi.org/10.1016/j.cose.2017.08.016
44. Sood SK, Mahajan I (2018) Fog-cloud based cyber-physical system for distinguishing, detecting and preventing mosquito borne diseases. Future Gener Comput Syst. https://doi.org/10.1016/j.future.2018.01.008
45. Stojmenovic I, Wen S (2014) The fog computing paradigm: scenarios and security issues. In: Proceedings of the 2014 federated conference on computer science and information systems, vol 2, pp 1–8. https://doi.org/10.15439/2014F503
46. Stojmenovic I, Wen S, Huang X, Luan H (2016) An overview of Fog computing and its security issues. Concurrency Comput Pract Exp 28:2991–3005. https://doi.org/10.1002/cpe
47. Sun Y, Lin F, Zhang N (2018) A security mechanism based on evolutionary game in fog computing. Saudi J Biol Sci 25(2):237–241. https://doi.org/10.1016/j.sjbs.2017.09.010
48. Wang H, Wang Z, Domingo-ferrer J (2018) Anonymous and secure aggregation scheme in fog-based public cloud computing. Future Gener Comput Syst 78:712–719. https://doi.org/10.1016/j.future.2017.02.032
49. Wang T, Zeng J, Lai Y, Cai Y, Tian H, Chen Y, Wang B (2017) Data collection from WSNs to the cloud based on mobile fog elements. Future Gener Comput Syst. https://doi.org/10.1016/j.future.2017.07.031
50. Wang T, Zhou J, Huang M, Alam Z, Liu A (2018) Fog-based storage technology to fight with cyber threat. Future Gener Comput Syst 83:208–218. https://doi.org/10.1016/j.future.2017.12.036
51. Wang Y, Uehara T, Sasaki R (2015) Fog computing: issues and challenges in security and forensics. Proc Int Comput Softw Appl Conf 3:53–59. https://doi.org/10.1109/COMPSAC.2015.173
52. Xiong C, Xiang R, Li Y, Han X, Du H (2018) Large-scale image-based fog detection based on cloud platform. Multimed Tools Appl. https://doi.org/10.1007/s11042-017-5597-6
53. Yang R, Xu Q, Ho M, Yu Z, Wang H, Zhou L (2018) Position based cryptography with location privacy: a step for Fog computing. Future Gener Comput Syst 78:799–806. https://doi.org/10.1016/j.future.2017.05.035
54. Yaseen Q, Aldwairi M, Jararweh Y, Brij MA (2017) Collusion attacks mitigation in internet of things : a fog based model. Springer Science + Business Media, LLC 2017, October. https://doi.org/10.1007/s11042-017-5288-3
55. Yi S, Qin Z, Li Q (2015) Security and privacy issues of fog computing: a survey. In: 10th International conference on wireless algorithms, systems, and applications, pp 685–695. https://doi.org/10.1007/978-3-319-21837-3_67
56. Zahra S, Alam M, Javaid Q, Wahid A, Javaid N, Ur S et al (2017) Fog computing over IoT: a secure deployment and formal verification. IEEE special section on recent advances in computational intelligence paradigms for security and privacy for fog and mobile edge computing 5:27132–27144. https://doi.org/10.1109/ACCESS.2017.2766180
57. Zhang P, Chen Z, Liu JK, Liang K, Liu H (2018) An efficient access control scheme with outsourcing capability and attribute update for fog computing. Future Gener Comput Syst 78:753–762. https://doi.org/10.1016/j.future.2016.12.015
58. Zhang P, Liu JK, Yu FR, Sookhak M, Au MH, Luo X (2018) Human-driven edge computing and communication: a survey on access control in fog computing. IEEE Commun Mag 55:144–149. https://doi.org/10.1109/MCOM.2018.1700333

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.