IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 21, 2020, accepted April 5, 2020, date of publication April 22, 2020, date of current version May 7, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2989456

Systematic Review on Security and Privacy Requirements in Edge Computing: State of the Art and Future Research Opportunities

MUKTAR YAHUZA[1,2], MOHD YAMANI IDNA BIN IDRIS[1,3], (Member, IEEE), AINUDDIN WAHID BIN ABDUL WAHAB[1,3], (Member, IEEE), ANTHONY T. S. HO[4], (Senior Member, IEEE), SULEMAN KHAN[5], (Member, IEEE), SITI NURMAYA BINTI MUSA[6], AND AZNI ZARINA BINTI TAHA[7]

[1]Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur 50603, Malaysia
[2]Department of Computer Science, Yobe State University, Damaturu 620242, Nigeria
[3]Center for Mobile Cloud Computing, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur 50603, Malaysia
[4]Department of Computer Science, University of Surrey, Guildford GU2 7XH, U.K.
[5]Department of Computer and Information Sciences, Northumbria University, Newcastle-upon-Tyne NE1 8ST, U.K.
[6]Faculty of Engineering, University of Malaya, Kuala Lumpur 50603, Malaysia
[7]Center for Business Strategy and Policy, University of Malaya, Kuala Lumpur 50603, Malaysia

Corresponding author: Ainuddin Wahid Bin Abdul Wahab (ainuddin@um.edu.my)

This work was supported in part by the University of Malaya Impact Oriented Interdisciplinary Research Grant under Grant IIRG008A,B,C-19IISS, and in part by the Ministry of Education-Fundamental Research Grant Scheme under Grant MOE-FRGS-FP072-2019A.

ABSTRACT Edge computing is a promising paradigm that enhances the capabilities of cloud computing. In order to continue patronizing the computing services, it is essential to conserve a good atmosphere free from all kinds of security and privacy breaches. The security and privacy issues associated with the edge computing environment have narrowed the overall acceptance of the technology as a reliable paradigm. Many researchers have reviewed security and privacy issues in edge computing, but not all have fully investigated the security and privacy requirements. Security and privacy requirements are the objectives that indicate the capabilities as well as functions a system performs in eliminating certain security and privacy vulnerabilities. The paper aims to substantially review the security and privacy requirements of the edge computing and the various technological methods employed by the techniques used in curbing the threats, with the aim of helping future researchers in identifying research opportunities. This paper investigate the current studies and highlights the following: (1) the classification of security and privacy requirements in edge computing, (2) the state of the art techniques deployed in curbing the security and privacy threats, (3) the trends of technological methods employed by the techniques, (4) the metrics used for evaluating the performance of the techniques, (5) the taxonomy of attacks affecting the edge network, and the corresponding technological trend employed in mitigating the attacks, and, (6) research opportunities for future researchers in the area of edge computing security and privacy.

INDEX TERMS Edge computing, edge computing attacks, systematic review, security and privacy requirements.

I. INTRODUCTION

Edge computing paradigm is developed with the intention of overcoming the drawbacks associated with cloud computing. In the edge computing, the edge network stands between the cloud and the end-users, thereby, bringing cloud resources very closed to the end-users [1]. This consequently provides tremendous real-time data analysis, reduce latency, low operational cost, high scalability, and improve the quality of services. The most challenging problem affecting the success of edge computing is a breach in the security and privacy of most of the components associated with it. This survey study

The associate editor coordinating the review of this manuscript and approving it for publication was Abdullah Iliyasu.

considers eight security and privacy requirements of a typical edge computing network. Security and privacy requirements can be referred to as the measure of the capabilities and functions that a system should achieve for eliminating the security and privacy vulnerabilities [2]. When the requirements are satisfied, the system complies successfully with the imperative private and secure targets, as well as relevant regulatory guidance [3]. The requirements include Privacy-Preservation, Confidentiality, Authenticity, Attack Detection, Integrity, Availability, Nonrepudiation, and Reliability. The detail of each requirement will be discussed in section III.

Many survey studies discussed the security and privacy issues in edge computing; however, most of these previous studies systematically overlooked the investigation on the security and privacy requirements in the edge computing network. In addition, research on the state of the art curbing techniques with the corresponding technological methods was also missing in the previous survey studies. In [4], Zhang *et al.* presented a survey on security and privacy issues in edge computing, however, only cryptography-based technologies that considered confidentiality requirements were highlighted. In [5], Rodrigo and his team analyzed and surveyed the security threats associated with the various edge computing related paradigms, such as fog computing, and mobile edge computing. However, the survey considered techniques related to authenticity requirement, whereas, less attention was given to other requirements. Guan *et al.* [6] discussed the main data flow in the energy sector, nevertheless, their survey work focused only on security and privacy issues in the area associated with the application of edge computing in the electricity sector. Rapuzzi and Repetto [7] likewise, reviewed the limitations of current cyber-security paradigms associated to the evolving fog/edge schemes. The survey work aimed at representing a basics for the design of innovative cyber-security methods, nonetheless, a thorough investigation of the security requirements was missing. Shirazi *et al.* [8] in another survey highlighted the need to come up with new security curbing strategies in the emergent area of edge/fog computing, and to investigate them in their new computing applications.

The various survey studies have laid a tangible foundation in understanding security and privacy issues in edge computing. However, most of these studies provided limited information with respect to the security and privacy requirements in the edge computing network. Besides, most of the work rather discussed partially or conducted the review when the problem was at an early stage. This review work will recapitulate the existing state of the art security and privacy requirements, as well as the trend of the technological methods employed by the techniques for curbing the associated threats in the edge computing for future researchers to follow. A systematic review protocol that will specify all the relevant stages necessary for achieving the aim and objectives of the study will be developed and considered from the initial stage before starting the process of data abstraction. This process will ensure impartial data search and retrieval. The contribution of this review work will be attained by answering the following research questions:

1) What are the categories of security and privacy requirements in the edge computing network?
2) What techniques are proposed for ensuring the requirements identified?
3) What trend of the technological methods are employed by the identified techniques?
4) What are the suitable evaluation metrics employed in assessing the performance of the techniques?
5) What are the categories of attacks affecting edge computing networks, together with the corresponding mitigating technologies?
6) What are the future research opportunities available for researchers working in the area of security and privacy of edge computing?

The remaining part of the paper is categorized as follows: Overview of edge computing similar paradigms (Post-Cloud Computing Paradigms) will be given in Section II, the overview of security and privacy requirements in edge computing will be stated in Section III, Section IV will highlight the methodology for conducting the systematic literature review, Data analysis will be given in Section V, the discussion of the reviewed result will be given in Section VI, Section VII will highlight the research open issues, and conclusion will be finally given in Section VIII.

II. OVERVIEW OF EDGE COMPUTING SIMILAR PARADIGMS

This section will introduce the edge computing similar paradigms, which are otherwise known as post-cloud computing paradigms. This includes Edge computing, Fog computing, Mobile Edge Computing (MEC), Cloudlet computing, Mist computing, and Dew computing. The post-cloud computing paradigms are used interchangeably by most researchers, although, they are not exactly the same. Therefore, this section compares and contrasts between the post-cloud paradigms, and clarify the similarities and differences that are ignored by most researchers. The post-cloud paradigms are all developed with the intention of overcoming the weaknesses of cloud computing for not satisfying the requirements of internet-of-things (IoT) and next-generation 5G networks. The most important requirements include real-time and distributed data processing, low latency, mobility support, quick response of wireless sensors and actuators, etc. Although the post-cloud computing paradigms have been developed by different organizations with different ideas, the principle of bringing cloud services closer to the end-user (network edge) is common. Table 1 summarizes the similarities and differences between the post-cloud computing paradigms.

In all of the post-cloud computing paradigms, end-users and other IoT devices are the main target for security and privacy breaches, because of their inability to establish explicit trust for other devices, and also their inability to establish a trustworthy connection. Generally, security and privacy need

TABLE 1. **Relationship between the edge computing similar paradigms.**

PROPERTIES	POST-CLOUD COMPUTING PARADIGMS					
	EDGE COMPUTING	FOG COMPUTING	MOBILE EDGE COMPUTING	CLOUDLET COMPUTING	MIST COMPUTING	DEW COMPUTING
SECURITY MEASURES	Should be applied to the edge devices because they are deployed in an environment with minimal protection [10]	Should be applied to participant nodes (Fog nodes) because they are deployed in decentralized locations where protection is minimal [10-13]	Should be applied to edge network equipment because they are deployed in an environment with minimal protection (e.g. RAN) [10]	Should be applied to participant nodes [10]	Should be applied to IoT(End-User) devices [10]	Should be applied to IoT(End-User) devices [14]
DEVELOPERS	The Pacific Northwest National Laboratory (PNNL) [4]	CISCO, 2011[14-16]	ETSI, 2014[15]	Carnegie Mellon University, founded by Nokia, Huawei, IBM, Intel, NTT DoCoMo, Vodafone 2013[15, 17, 18]	CISCO [19]	Started in 2012, but reflected in 2013 to 2015 [14]
DISTANCE FROM CLOUD	Away from cloud and closer to the end-users when compared to the other post-cloud computing paradigms[10, 20]	Away from the cloud and relatively close to the end-users when compared to the other post-cloud computing paradigms [10, 20-22]	Away from the cloud and at the vicinity of the mobile devices [10, 23, 24]	Away from cloud and closer to mobile devices when compared to the other post-cloud computing paradigms [10, 15, 25]	Away from the cloud and the closest to end-users when compared to the other post-cloud computing paradigms [10, 26]	Away from cloud and closer to IoT when compared to the other post-cloud computing paradigms (End-User) devices
GEOGRAPHICAL DISTRIBUTION	Distributed datacenters[15]	Distributed fog nodes [15]	Dense and disperse infrastructures [15, 24]	Distributed virtual machines servers [15]	Distributed microcontrollers of the embedded nodes	Distributed smaller servers embedded on the end-users' computer [27, 28]
NATURE OF APPLICATION	Moderate computation with lower latency [10, 15]	High computation with low latency [15]	Moderate computation with very low latency [10, 24]	Higher computation with lower latency when compared to the other post-cloud paradigm [10, 15]	Dispersed processing on IoT devices [10]	N.A
TYPE OF SERVICES	Local [10, 15]	Less Global than Cloud Computing [10, 15]	Local [10, 15, 24]	Local [10, 15]	Local[10]	Local
CONNECTIVITY	WAN, WLAN, LAN, Wi-Fi, Cellular, Zigbee, and can operate with no or relatively low connection [10, 15, 29]	WAN, LAN, WLAN, Wi-Fi, Cellular, Zigbee, and can operate with no or relatively low connection [10, 11, 15]	WAN, Cellular, and can operate without network or connected via RAN[10, 15, 24]	WAN, WLAN, Wi-Fi, LAN, Cellular, and can operate with no or relatively low connection, but most of the time requires connection [10, 24, 30]	LAN, Bluetooth, Wi-Fi, Cellular, Zigbee and can operate with relatively low connection, but there must be a connection[10]	Accessible by end-users even in the absence of network [27]
MOBILITY	Supported [15, 31]	Supported [11, 15, 31]	Supported [15]	Supported [15]	Supported [10]	Supported [14]
COMPUTING RESOURCES	Moderate [10]	Limited [10]	Moderate [10, 24]	Moderate [10, 24]	Limited [10]	Limited
SERVER NODES LOCATION	Very near to edge devices[10, 15]	At relatively near or at designated locations [10, 11, 15]	Located at the surrounding area of the mobile devices [10, 24]	Located near mobile devices[10]	Located near end-devices	N.A
DRIVING FACTOR	IOT [15]	IOT [15]	Mobile IOT [15]	Mobile IOT [15]	IOT [10]	IOT [27]
TARGETED USERS	General [10]	General [10]	Mobile devices [10]	Mobile devices [10]	General [10]	General [27]

to be provided in every layer of the post-cloud computing networks [4]. Barika Pace, a research director highlighted that "Each IOT device in post-cloud computing network is configured in a different way which leads to having a different version with different vulnerabilities, and consequently causes problems" [9]. Another issue that leads to the security and privacy breach of the post-cloud computing paradigms, with the exception of MEC is that the data and computational tasks of end-users are communicated through a decentralized edge network.

According to Duncan Pauly, a CTO at Edge Intelligence, "The security and privacy risks associated with post-cloud

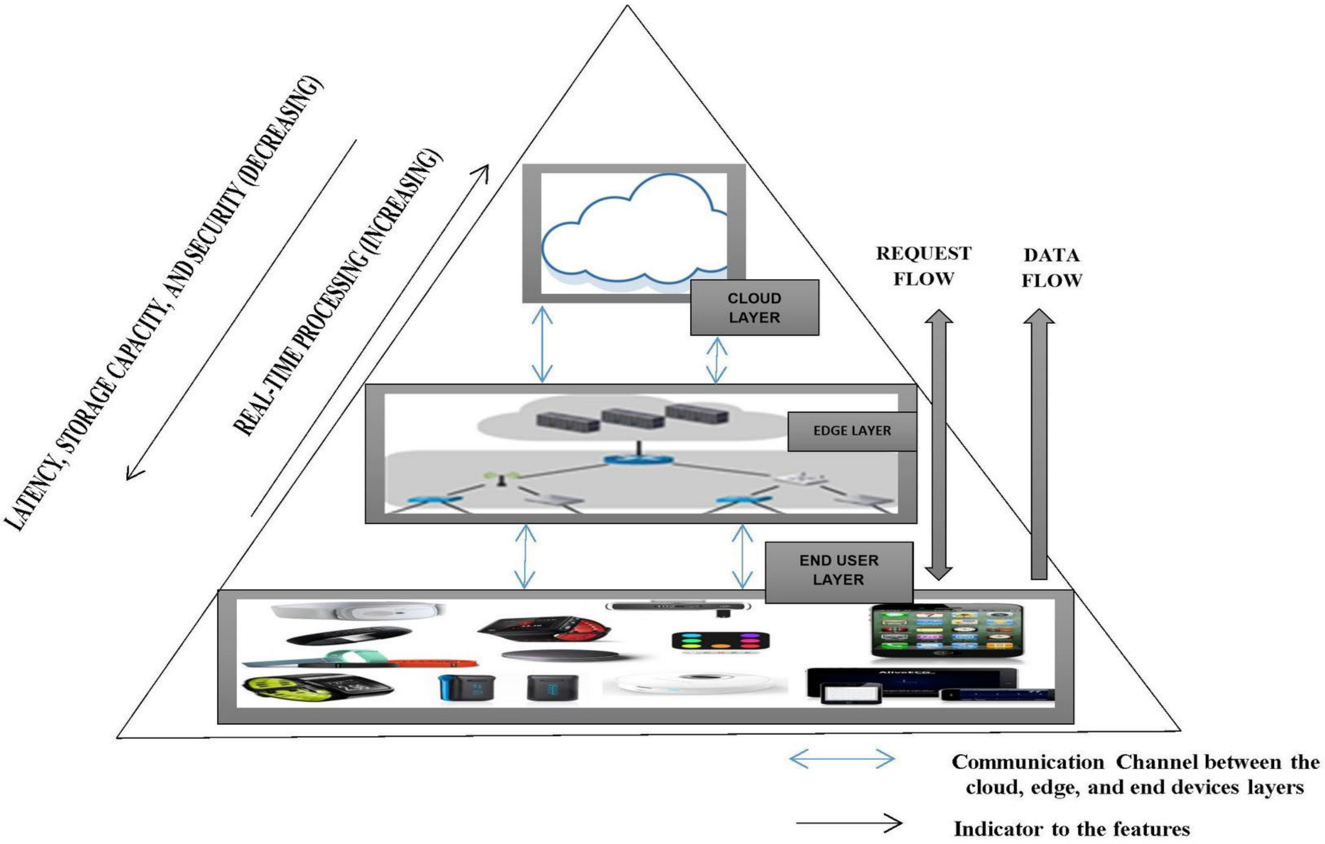
LATENCY, STORAGE CAPACITY, AND SECURITY (DECREASING)
REAL-TIME PROCESSING (INCREASING)
CLOUD LAYER
EDGE LAYER
END USER LAYER
REQUEST FLOW
DATA FLOW
Communication Channel between the cloud, edge, and end devices layers
Indicator to the features

FIGURE 1. Edge computing architecture.

computing paradigms are quite different from a cloud environment, because all the data in the cloud are stored or process in a single or small number of locations, whereas in post-cloud computing paradigms, data is decentralized'' [9]. Thus, sensitive data associated with end-user can be compromised. Furthermore, the offloaded data and other complex computational tasks together with some cloud resources are stored at the network edge, which is more vulnerable than the cloud itself [10].

Shane MacDougall, a senior security engineer at networking and cyber-security services company Mosaic452, argued that ``The best practice for ensuring security and privacy in post-cloud computing networks is to provide an equal amount of protection to all of the edge/Fog and other related nodes as the remaining part of the network'' [9]. In another hand, the worst practice of ensuring post-cloud computing security and privacy is to employ the traditional security controls, for example, using only antivirus and firewalls to protect the edge devices. Joseph Carson, the chief security scientist at Thycotic, an access management technology provider said, ``In post-cloud computing, the organization's data are no longer flowing through their internet connection, nor via their corporate firewall, so there is a need to secure and protect each edge device as if it is a door to their network'' [9]. Another poor practice for ensuring security and privacy in edge computing is employing cloud-based security models. Therefore, for proper handling of security and privacy in the post-cloud network, certain security and privacy requirements need to be considered in the process of enabling smooth operation of the entire network. This review work will concentrate only on the edge computing security and privacy requirement, which will be discussed in section III.

The typical architecture of edge computing is illustrated in Fig. 1, while the architectures of the other edge similar paradigms are illustrated in Fig. 2. More details on the post-cloud computing paradigms and their comparison can be found in the work of Yousefpour *et al.* [11]. Fig. 1 depicts the typical 3-layer architecture of an edge computing paradigm. The edge layer stands in between the cloud and the end-device layer. It can be seen from the Fig.1 that the latency decreases significantly from an edge network layer to an end-devices layer when compared to that of the cloud layer and end-devices layer. This is an important feature of an edge computing paradigm. The security decreases drastically when moving away from the cloud layer to an edge layer and then to an end-device layer, which is as the result of distributed nature of the edge network. It can also be observed

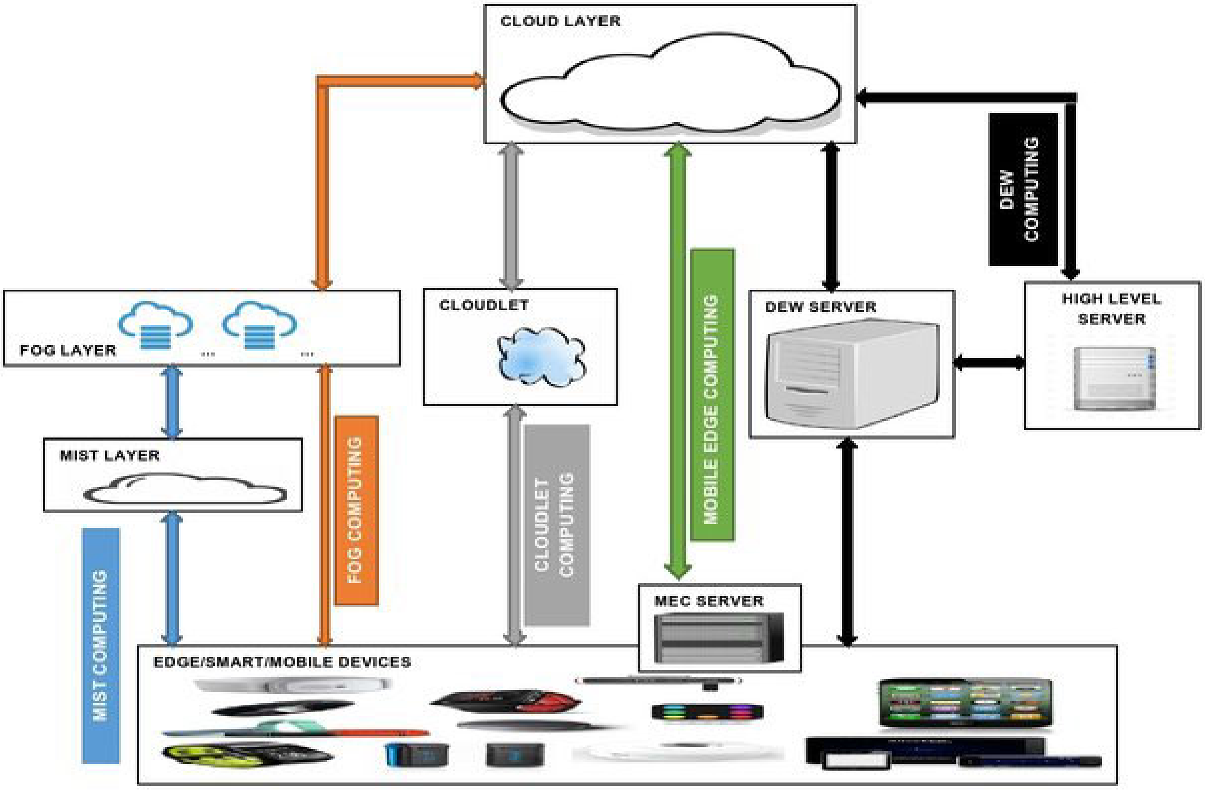

FIGURE 2. The architecture of the edge similar paradigms.

that the storage capacity decreases drastically from the cloud layer to the edge layer and then to the end-device layer. The real-time processing decreases dramatically when moving from end-devices to an edge layer and then to the cloud layer. Data flows from end-devices to edge layer for storage or processing, then to the cloud layer when long term storage is required. Requests in the edge computing network flow in two directions, as depicted in Fig. 1.

Similarly, in Fig. 2, fog computing consists of fog nodes that are distributed over geographical locations, very close to end-user devices. The overall computation process is done at the edge of the network, very close to the data sources [12]. The architecture of mobile edge computing (MEC) is also depicted in Fig. 2. As shown, the MEC computing consists of MEC servers that are located in the vicinity of the mobile users. Thus mobility is highly supported, and latency is relatively lower than the remaining post-cloud computing paradigms. Fig. 2 also illustrates the architecture of the cloudlet computing. As shown in Fig. 2, cloudlet computing consists of a relatively small mobility support cloud called cloudlet located close to the mobile end-users. The cloudlet is connected to the faraway cloud, and it brings computational resources directly into mobile devices with relatively low latency. Cloudlets are installed on distributed virtual machines servers connected together by the LAN network, on which mobile devices can upload high computational tasks. Cloudlet does not have to be fixed infrastructures close to the end-devices, but may rather be accessible through the wireless LAN network.

The architecture of Mist computing is also shown in Fig. 2. As depicted in the figure, data processing is at the extreme edge of the network because fog nodes stand between the cloud layer and the mist layer, resulting in less network delay, reduced latency, as well as bandwidth utilization, when compared to the remaining post-cloud paradigms. Thus, it can be said that, in Mist computing, computation is pushed further to the network edge. Therefore, devices at the edge, such as sensors and actuators are involved in the computing process, which is not the case when compared to the other post-cloud computing paradigms. This allows the computation to be performed by microcontrollers of the embedded nodes [27]. Fig. 2 also shows the architecture of the dew computing paradigm. It can be seen that the dew computing consists of dew servers that allow the cloud information to always be available on end-devices, connected to the nearby dew server, so that cloud data will be available even in the absence of internet service [28], [33]. Unlike cloudlet computing, dew computing employed relatively high-level servers, which provide services similar to that of cloud and also synchronizes its database to the database of the cloud [34]. Thus providing services independent to the cloud, and also in collaboration with the cloud [29].

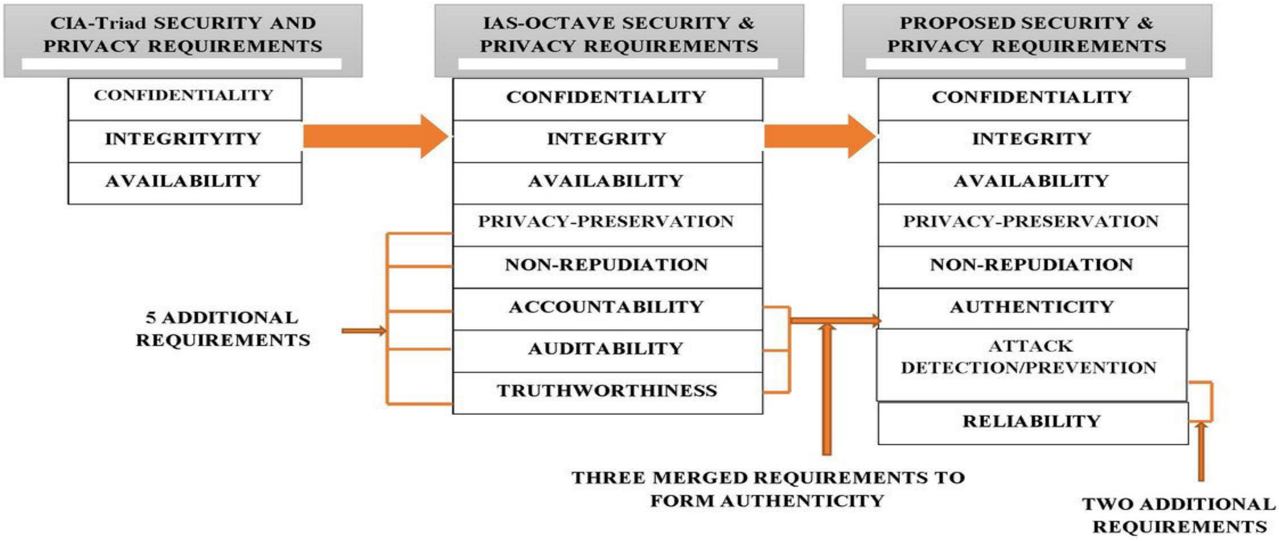
CIA-Triad SECURITY AND PRIVACY REQUIREMENTS
CONFIDENTIALITY
INTEGRITYITY
AVAILABILITY
IAS-OCTAVE SECURITY & PRIVACY REQUIREMENTS
CONFIDENTIALITY
INTEGRITY
AVAILABILITY
PRIVACY-PRESERVATION
NON-REPUDIATION
ACCOUNTABILITY
AUDITABILITY
TRUTHWORTHINESS
5 ADDITIONAL REQUIREMENTS
PROPOSED SECURITY & PRIVACY REQUIREMENTS
CONFIDENTIALITY
INTEGRITY
AVAILABILITY
PRIVACY-PRESERVATION
NON-REPUDIATION
AUTHENTICITY
ATTACK DETECTION/PREVENTION
RELIABILITY
THREE MERGED REQUIREMENTS TO FORM AUTHENTICITY
TWO ADDITIONAL REQUIREMENTS

FIGURE 3. Development of the security and privacy requirements in edge computing.

III. OVERVIEW OF THE SECURITY AND PRIVACY REQUIREMENTS IN EDGE COMPUTING NETWORK

In the traditional way, security and privacy requirements are categorized into three main groups referred to as CIA-Triad [35]. They include Confidentiality, Integrity, and Availability. However, due to the insufficiency of CIA-Triad to address new threats in the shared security environment (like edge computing), a comprehensive list of security and privacy requirements called IAS-Octave was formulated [36]. IAS-Octave can be utilized in edge computing due to its ability to address new threats in the shared environment. In the IAS-Octave categorization, Accountability, Auditability, Trustworthiness, Nonrepudiation, and Privacy-Preservation security requirements are added to the CIA-Triad, thus making a total of eight requirements. Considering the fact that Accountability and Auditability lead to Trustworthiness [37], [38], and also, Trustworthiness is highly related to Authenticity requirement [39], the three requirements can be merged together to form Authenticity. Additionally, the security and privacy requirements of edge computing, which are not included in the IAS-Octave when compared with the reviewed studies under the edge computing perspective are Attack Detection and Reliability. Therefore, in this paper, edge computing security and privacy requirements are proposed. They include Confidentiality, Integrity, Availability, Privacy-Preservation, Nonrepudiation, Authentication, Attack Detection, and Reliability. Table 2 illustrates the description of the proposed edge computing security and privacy requirements, which will be considered in the review work. Similarly, Fig. 3 illustrates the development of the security and privacy requirements from CIA-Triad to the proposed requirements.

TABLE 2. Description of the security and privacy requirements.

S/N	REQUIREMETS	DESCRIPTION
1	Confidentiality	It ensures that only genuine data owners and intended receivers have the right to access private information or data in the edge computing environment.
2	Integrity	This requirement ensures the delivery of data and information only to authorized edge devices without any form of modification.
3	Availability	It ensures that all the edge computing participants, including the edge nodes and end users are able to access all the services at any moment in time.
4	Privacy- Preserving	This requirement ensures that all the secret information for end users are kept undisclosed under trust and monitoring
5	Non-Repudiation	It ensures occurrence or nonoccurrence of any task. It guarantees that a user or edge node did not deny any accomplished action.
6	Authenticity	This requirement ensures careful monitoring, verification of edge computing participants' identity, and also establishment of trust among them.
7	Attack Detection	It ensures that the attacks associated with edge computing network are detected and eradicated accordingly.
8	Reliability	This requirement ensures that the genuine communicating edge computing entity believes with other genuine entity under sufficient and credible evidence

IV. METHODOLOGY

This review work employs a systematic review to ensure accurate and impartial data search and retrieval. A review protocol that specifies the search strategy, devising of inclusion and exclusion criteria in the selection of the articles to be considered or ignored respectively, and plan for analyzing the

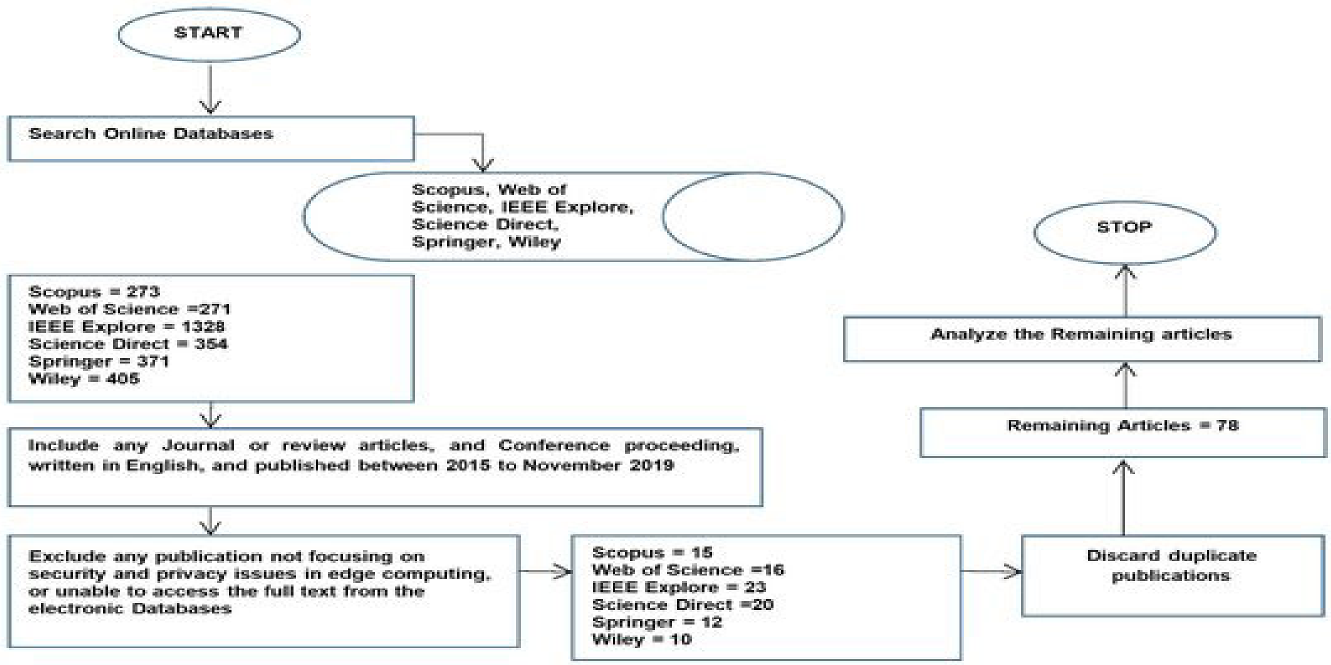
START
Search Online Databases
Scopus, Web of Science, IEEE Explore, Science Direct, Springer, Wiley
Scopus = 273
Web of Science =271
IEEE Explore = 1328
Science Direct = 354
Springer = 371
Wiley = 405
Include any Journal or review articles, and Conference proceeding, written in English, and published between 2015 to November 2019
Exclude any publication not focusing on security and privacy issues in edge computing, or unable to access the full text from the electronic Databases
Scopus = 15
Web of Science =16
IEEE Explore = 23
Science Direct =20
Springer = 12
Wiley = 10
Discard duplicate publications
Remaining Articles = 78
Analyze the Remaining articles
STOP

FIGURE 4. The methodological steps of the review work.

selected articles was developed from the initial stage before beginning the search process of literature and data extraction. The protocol was approved by one of the authors prior to its implementation. The steps involved in the methodology of the review work are illustrated in Fig. 4.

A. DATA SEARCH STRATEGY

A thorough search was conducted on all studies that focus on security and privacy issues in edge computing including both review and technical studies. The entire search was carried out through six prominent online electronic databases, which include: Scopus, Web of Science, IEEE-Explore, Science Direct, Springer, and Wiley. This is because they encompass publications from the major journal and conference proceedings, and as such, a reasonable sample that will represent the current state of knowledge in the area of edge computing privacy and security will be obtained. Restricting the search on the four mentioned online electronic databases implies that only a sample of the literature on the intended review is targeted.

Also, limiting the search to only computer science and information, computer science and theory, and engineering subject areas were made in order to limit the boundary of the review work. The initial search was made by filtering only conference, technical and review journal articles that were published between 2015 to November 2019. The search tip used in retrieving the articles include:

1) "Security and Privacy" AND "Edge Computing" OR "Security" AND "Edge Computing" AND "Trust" OR "Privacy" AND "Edge Computing"
2) "Secur*" AND" Privacy" OR "Trust" AND "Edge Computing."

TABLE 3. Inclusion and exclusion criteria.

INCLUSION CRITERIA	EXCLUSION CRITERIA
• An article is considered for inclusion if it is either a Journal or Conference paper to achieve the highest level of significance • An article is considered for inclusion if it is Published between 2015 to November 2019, to include the latest techniques employed in solving security and privacy issues in edge computing • It is written in English	• An article is considered for exclusion if it is not focusing on security and privacy issues in the edge computing area • An article is considered for exclusion if it is not fully accessible from the online electronic databases (Scopus, Web of Science, IEEE-Explore, Science Direct, Springer, and, Wiley)

A total of 273 articles from Scopus, 271 from Web of Science, 1328 from IEEE-Explore, 354 from Science Direct, 371 from Springer, and 405 from Wiley were obtained. A total of 3,002 articles were found. A scan was made on the title and abstract of the searched articles. After the scan, 2,730 articles found to be either beyond or not even related to the scope of the review work, and were completely removed. Inclusion and exclusion procedures were then applied to the remaining 272 articles for further selection. An article is considered for inclusion if it satisfies the inclusion requirement highlighted in Table 3, and it is excluded if it satisfies the exclusion criteria. After the full-text review of the remaining 272 retained articles, 96 fulfilled the inclusion requirements.

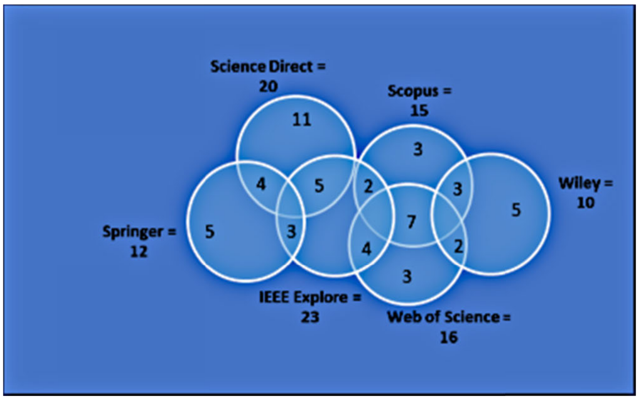

FIGURE 5. A diagram showing the distribution of the searched articles according to their respected database.

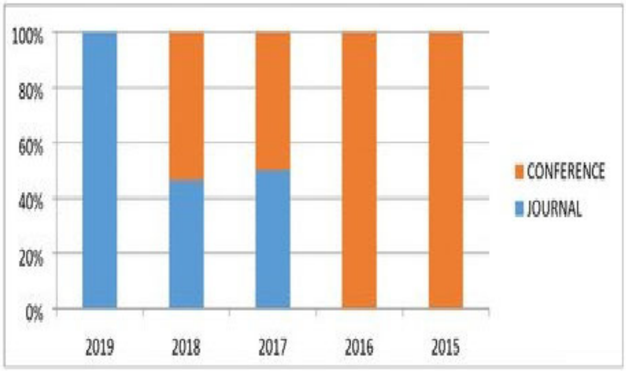

FIGURE 6. Percentage of the reviewed journal articles and conferences.

Again, duplicate articles are extracted and discarded, leaving a total of 78 articles. The distribution of the retained articles according to their respective databases is depicted in Fig. 5

B. DATA EXTRACTION

Relevant data that will answer the research questions were exhaustively abstracted from the 78 articles that fulfilled the inclusion criteria. The following items were documented: Authors, Year of publication, type of the article, the technique under a specific category of security and privacy requirement, the category of the technological methods employed, performance metrics used in evaluating the performance of the proposed technique, and the attacks considered by the techniques. Additionally, research opportunities are derived from the weaknesses of each identified techniques.

V. DATA ANALYSIS

In this section, all the studies that fulfilled the inclusion criteria will be systematically analyzed. The steps of the general data analysis will be described in sub-section A. Also, the analysis based on the proposed security and privacy requirements, which will answer the research questions will be given in sub-section B.

A. GENERAL DATA ANALYSIS

The review work examined 78 articles from various journals and conference proceedings across the four different electronic databases. Fig. 6 illustrates the percentage of journal articles and conference papers published between 2015 to November 2019. Based on the review findings, there is no visible journal publication between 2015 and 2016, which may be regarded as research on security and privacy on edge computing only gain popularity in the year 2016. 50% and 48% of 2017 and 2018 publications journal articles respectively. This may be due to the fact that researchers lately start developing interest in security and privacy issues in edge computing. In the year 2019, 100% of the publications from the review work are from journal articles. This may be because additional interests are diverted to the area of security and privacy in edge computing. However, conference papers may also be available in other electronic databases.

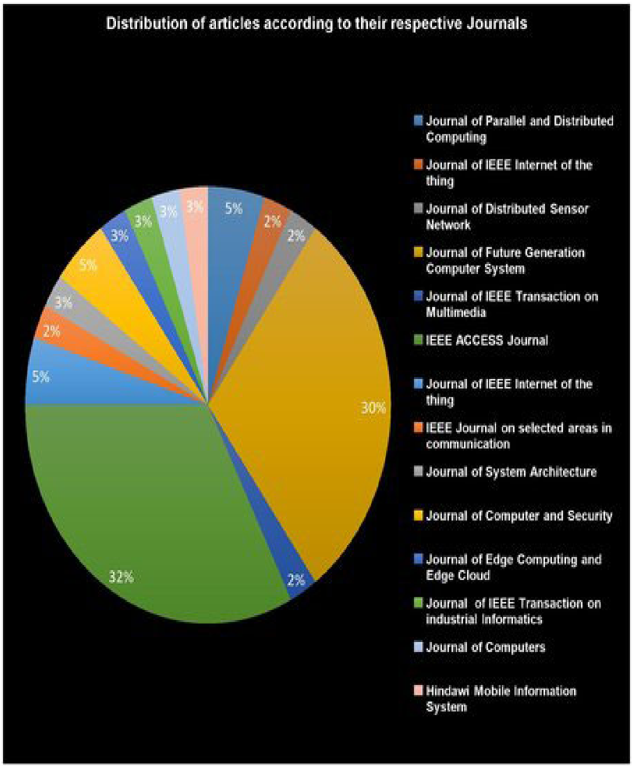

FIGURE 7. The distribution of the articles according to the journal that published them.

Fig. 7 shows the distribution of the articles according to the different journals spanning a broad range of disciplines. The majority of the articles were from the IEEE Access Journal (32%), followed by the journal of the Future Generation Computer System (30%). The next most prevalent journals are the Journal of Parallel and Distributed Computing, while IEEE Internet of the Thing Journal and Journal of Computer and Security, having 5% each. Journal of System Architecture, Edge Computing, and Edge Cloud Journal, and Journal of Distributed Sensor Network are having 3% each. However, Hindawi Mobile Information System Journal, the

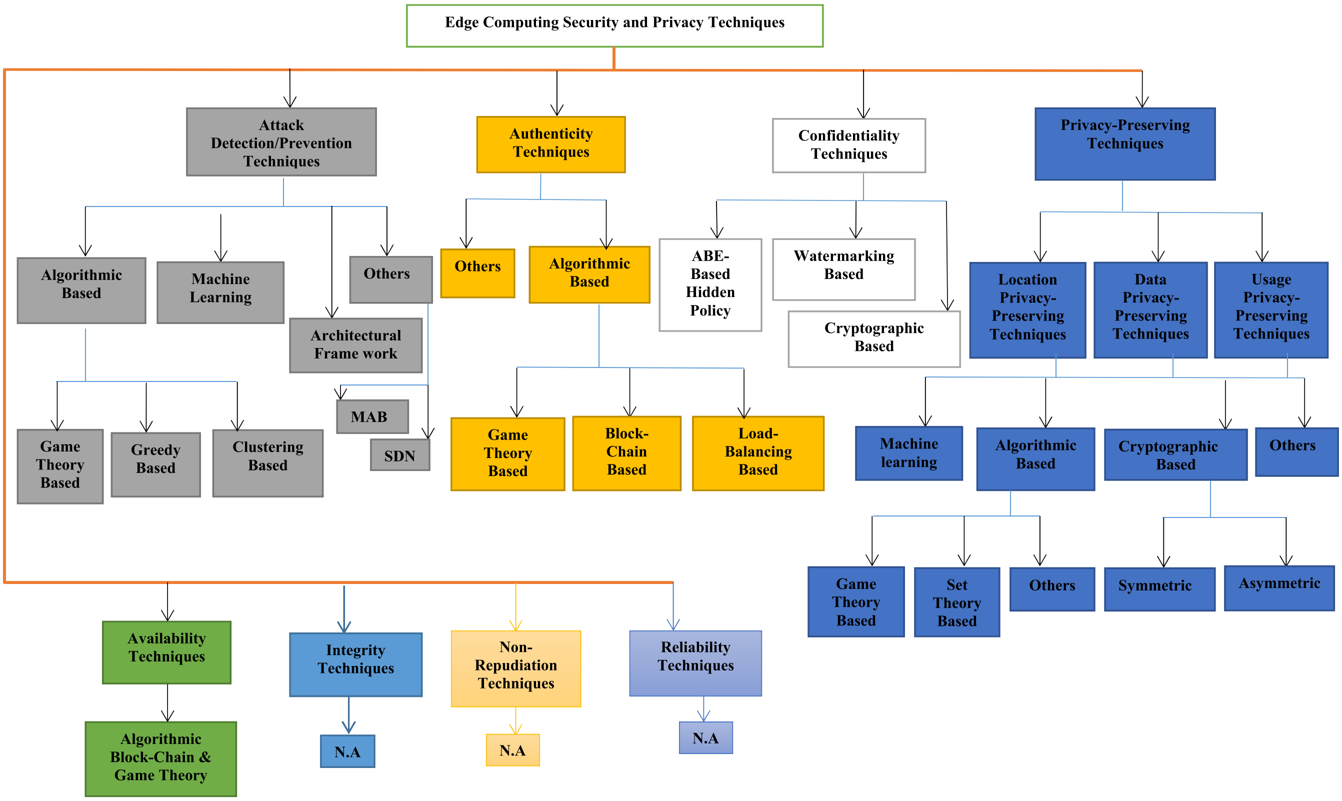

FIGURE 8. The taxonomy of the edge computing security/privacy curbing techniques and the technological trends.

Journal of Computers, Transaction and Industrial Informatics Journal, Journal of the Selected Area in Communication, and Journal of Transaction in Multimedia are all having 1% each.

B. DATA ANALYSIS BASED ON THE PROPOSED SECURITY/PRIVACY REQUIREMENTS

Subsection B(1) aimed at answering the research question 1 (RQ1) that focused on the classes of the security and privacy requirement in edge computing network, research question 2 (RQ2) that deliberates on the techniques proposed for ensuring the identified requirements, research question 3 (RQ3) that concentrates on the trend of the technological methods employed by the identified techniques, and, research question 6 (RQ6) that emphasizes on the research opportunities (gaps) for future researchers working in the area of security and privacy in edge computing. Research question 4 (RQ4) that focuses on finding the employed evaluation metrics assessing the performance of the identified techniques will be answered in Sub-section B (2). Similarly, research question 5 (RQ5) that highlights the attacks affecting edge computing network, with the corresponding technological curbing techniques will be explored in Sub-section B (3).

1) DATA ANALYSIS TO ANSWER RQ1, RQ2, RQ3, AND RQ6

In this section, the identified techniques that considered a specific category of security and privacy requirements are classified as depicted in Fig. 8. Additionally, Fig. 9 and Fig. 10 illustrate the classification of the techniques that consider more than one requirement, and the techniques that did not specify any of the proposed requirements respectively. Similarly, a summary of technique ideas under a given requirement is given in tables. In the tables, the description of the methodology, the technology employed, the used performance evaluation analysis, the advantages, and the disadvantages/gaps are given.

Table 4 reviews the techniques under Confidentiality requirement, Table 5 recapitulates the techniques under Privacy-Preservation requirement, Table 6 analyses the techniques under Authenticity requirement, Table 7 explores the techniques under Attack Detection requirement, Table 8 summarizes the techniques that considered the combination of both Authenticity and Privacy-Preservation, Table 9 reiterates the techniques that considered more than two requirements, and Table 10 summarizes the techniques that did not specify any of the proposed requirements.

Based on the review work, a technique that considers the Integrity requirement alone could not be established, except in combination with other techniques. Furthermore, findings show that only one study considered the availability requirement. Authors in [40] applied both block-chain and game theory methods to overcome the attack on edge servers by mobile devices in the edge computing network. A punishment scheme based on the active record of a Block-Chain

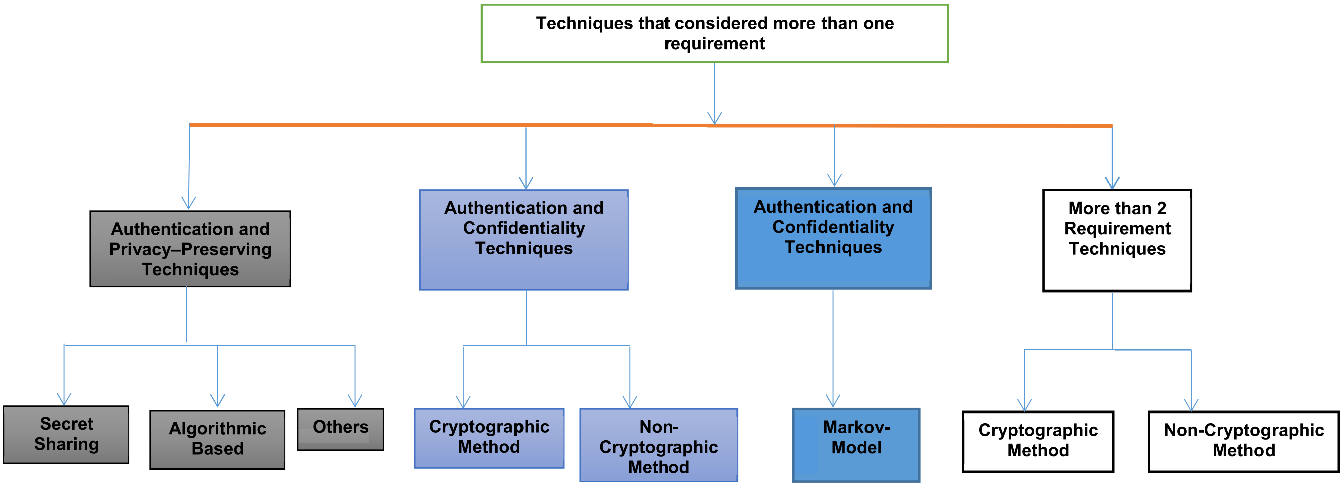
Techniques that considered more than one requirement
Authentication and Privacy–Preserving Techniques
Authentication and Confidentiality Techniques
Authentication and Confidentiality Techniques
More than 2 Requirement Techniques
Secret Sharing
Algorithmic Based
Others
Cryptographic Method
Non-Cryptographic Method
Markov-Model
Cryptographic Method
Non-Cryptographic Method

FIGURE 9. The classification of techniques that considered more than one requirements.

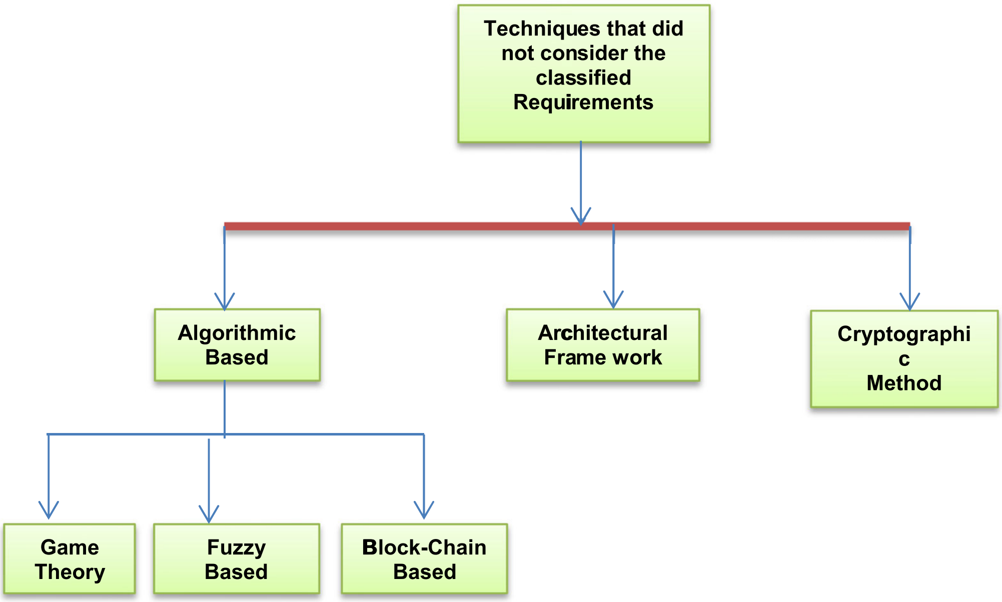

FIGURE 10. The classification of techniques that did not consider any of the proposed requirement.

was proposed. A block-chain security game is formulated by considering the interaction between the edge server and the mobile devices. The mobile devices either send a request to the server to obtain a real-time service or to launch an attack. Nash equilibrium is employed to determine the exact intention of the mobile device of either service request or attack. The scheme improved the network security performance by decreasing the attack rate of the server by 66.7% as compared to other similar techniques. Mathematical analysis is employed in evaluating the performance of the block-chain security game. Furthermore, according to the review work, a technique that considered Nonrepudiation requirement either alone or in combination with other requirements is not found.

Likewise, a technique that considers the Reliability requirement alone is also not found, except in combination with Authenticity requirements. Han, B., and his colleague in [41] devised an edge computing security technique based on the Markov model. The objective is to propose a decentralized authentication scheme that can provide flexible and low-cost authentication, which is aware of the context information of user devices and other network elements. They introduced trust architecture with cognitive access management. A context-aware mechanism, which synchronizes and reduces the backhaul network traffic, was designed. A simulation was conducted to validate the effectiveness of the technique. The proposed scheme was successful in maintaining the balance between network operating costs and

TABLE 4. Summary of the confidentiality techniques.

REFERECES	DESCRIPTION	TECHNOLOGY EMPLOYED	PERFORMANCE ANALYSIS METHOD	ADVANTAGES	LIMITATION/GAP
[45]	To provide Access control over Encrypted Data in the edge computing environment, the authors focused on ensuring confidential channels for key distribution in edge computing. They proposed Proxy-Aided Cipher Text-Policy ABE (PA-CPABE) that offloads the majority of the decryption computation to the trusted edge data centers so that no channel will be needed for key distribution.	ABE policy hidden methods	Prototype Implementation	• No channel is needed for key distribution • The decryption cost for PA-CPABE is negligible when compared to the ordinary ABE Scheme.	A method that will reduce the high computational overhead associated with ABE policy hidden technique needs to be designed.
[46]	The objective of the study is to revoke users' secret keys after being compromised and to minimize communication and computation overheads to attain lightweight requirements. The author proposed Cipher Policy-ABE (CP-ABE) that ensures the confidentiality of users' private information when shared within the edge computing network. Every authorized user is assigned with an ID, and the total IDs of the users are embedded in the private key that will be used for data encryption. Therefore, the only user whose ID corresponds to the ID sets can decrypt the cipher text. In any event, when the ID of a user is compromised, the data owner simply removes the ID of the affected user from the ID set and encrypts the information again. Thus, any compromised user will be automatically removed without affecting other users.	ABE policy hidden methods	Informal Security Proof, and Prototype Implementation	The scheme satisfied all the three attributes of fully policy hidden CP-ABE that include; partially policy-hidden, direct revocation of compromised users, and light-weightiness.	A method that will reduce the high computational overhead associated with ABE policy hidden technique needs to be designed
[47]	With respect to the protection of multimedia contents ownership in edge computing, the authors proposed a zero watermarking together with visual cryptography. To develop the Biometric security of face images and to prevent copying of multimedia contents in an edge computing network, the authors captured a face image using the Viola-Jones algorithm and convert it to grayscale. A DWT of the converted image is zero-watermarked with a unique ID. Visual cryptography is then applied to the watermarked image. At the receiver end, visual decryption is applied to obtain the watermarked image. Lastly, watermark detection and face recognition are applied to verify the image.	Watermarking Method	Real Dataset	The proposed scheme does not temper with the facial image, and therefore has no effect on the recognition rate.	There is a need to secure other multimedia contents, e.g. Audio and Video, not only face image.
[48]	The objectives of the scheme are to analyze 3 AES implementations with first-order resistant masking in edge computing, and to propose a new scalable collision attack with the common application and high efficiency, which can be applied to the 3 AES implementation. The authors considered the situation when little or no concern is given to the linear layer of S-Boxes of AES algorithm when trying to recover the secret key applied in edge computing for ensuring data confidentiality. Firstly, a new type of collision attack that uses leakages from linear layers and capable of breaking any masking schemes is proposed. Secondly, a scalable collision attack which is used to mask the S-Boxes is also proposed.	Cryptographic Based (AES Algorithm)	Prototype Implementation	• The proposed collision attack is efficient in reducing the number of power traces when compared to other collision attacks • With the improvement in linear collision attack, the signal to noise ratio was significantly reduced.	There is a need for collision attack to be applied to the general masking strategies of a symmetric cipher.

reliability. However, the security mechanism needs to be evaluated in accordance with the 5G network, which may be in respect of the corresponding application of the local authentication.

Moreover, two studies from the review work devised techniques that ensured both Authenticity and Confidentiality requirements. They are classified according to the employed methods as shown below:

a: CRYPTOGRAPHIC BASED TECHNIQUES

Ali *et al.* [42] proposed a multimodal authentication scheme by employing biometric encryption. Biometrics including speech and face image are encrypted using portable devices. Decryption occurs in the cloud, where each user is authenticated. The majority voting technique is used for a final decision about the user identity. The objective of the scheme is to propose a multimodal authentication system using encrypted biometrics for edge-centric cloud network. The proposed scheme can successfully hide the identity of users and, in the end, retrieve the biometrics accurately with an errorless authentication. However, the security involved is not strong because the scheme cannot generate the secret shares of the biometric templates.

The process of combining cryptography and biometric in securing user's information is termed as biometric-cryptography [43], [44]. The higher level of security is achieved with biometric-cryptography since the biometric templates assist the cryptographic process to encrypt and decrypt the information involved [43]. There are two different types of biometric-cryptography. The first one is called a biometric key release, which involves the occurrence of biometric matching in extracting the cryptographic key [43]. In the second type called biometric key generation templates, both biometric template and cryptographic key are combined together [43], hence no matching is required as in the first type.

b: NONE-CRYPTOGRAPHIC BASED TECHNIQUES

Chen *et al.* [45] proposed a none-cryptographic security scheme, where a password is not required for authentication purposes. A signal fingerprint feature, generated by the radiation of radio frequency of terminal devices (RF Fingerprint) is used by edge devices for the authentication process. In the proposed scheme, no password authentication is required, and as such, the scheme is more reliable when compared to the traditional cryptographic protocols. The author's employed simulation in evaluating the performance of the scheme, employing signal to noise ratio (SNR) as metrics.

RF fingerprints are distinctive features implanted in electromagnetic waves usually emitted by transmitters [46], [47]. The RF fingerprints aimed at serving the same purpose

TABLE 5. Summary of the privacy-preserving techniques.

REFERENCE	DESCRIPTION	TECHNOLOGY EMPLOYED	PERFORMANCE ANALYSIS METHOD	ADVANTAGES	LIMITATION/GAP
[49]	The technique is proposed to safeguard data transmission over a less secure wireless sensor network. The scheme supports nearest neighbor sparse representation and Vector Machine classifiers to analyze the new problem of privacy-preserving classification under the new edge computing scenario.	Machine Learning	Synthetic Dataset	• The proposed system is proficient for applying for differential privacy protection in the feature selection stage • The proposed scheme ensures protection against reconstruction attacks with a reasonable impact on classification accuracy	There is a need to balance privacy and efficiency, apart from establishing the tradeoff between privacy and utility preservation.
[50]	To analyze the limitations of typical task allocation and obfuscation schemes, and also to model the location obfuscation sub-issue through issue decomposition as a leader-follower game between the designer of location obfuscation mechanism and the potential attacker. The authors introduce an edge node into the edge network to prevent the untrusted crowd-sensing server from accessing users' private data. Both joint privacy protections, as well as task allocation problems, were solved by means of issue decomposition.	Game Theory Algorithm	Simulation (Computer Simulation Experiments)	• The study maximizes task acceptance rate and provided privacy guaranty by formulating the optimization issue after comparing user-centric and task-centric allocation approaches • The study solved joint privacy protection and Task allocation problems	There is a need for fine-grain security features, and therefore, tracking accuracy, and privacy protection level performance metrics need to be evaluated.
[51]	The authors consider the challenge associated with sensing-based mobile edge computing applications in managing data privacy without certifying tradeoff between performance and accuracy, in order to develop a novel framework for the proposed scheme for authentication in social sensing-based edge computing with reference to ring signatures, and also to develop a bottom-up approach for negotiating the ring compositions based on an enhanced clustering algorithm, a framework that utilizes a ring signature was proposed.	Game Theory Algorithm	Simulation (Ns-3), Prototype Implementation (Single Board Computer), and Real Dataset	With the proposed scheme, the management of privacy and security can be done by the edge devices without the need of any third-party trusted authority	The scheme is unable to establish consensus among the connected devices in a situation where there is no time to deploy a block-chain.
[52]	The authors proposed a HFRS-PP technique that combines filtration and rough set theory algorithms to distinguish the valid reviews from malicious reviews for the next filtration, in order to design a secure recommender system on the interconnected network that will minimize the privacy leakage of users selecting their desired product in the network, and to prevent leaking of users' privacy information in edge computing, thus, ensuring real-time stability and accuracy of query results.	Set Theory Algorithm	N/A	Apart from ensuring security and privacy, the proposed system also improves the network workload and delay, and also ensure end-user satisfaction	Security and efficiency analysis need to be conducted in order to evaluate the performance of the technique.
[53]	The authors identified both location and usage privacy-preserving that was initiated by the wireless task offloading in mobile edge computing. They proposed a privacy-aware task offloading scheduling algorithm based on the CMDP framework. They also proposed a privacy-aware task offloading scheduling algorithm based on Markov decision process.	Other Algorithm (Markov Decision Process and Task Offloading Algorithm)	Simulation (Computer Simulation Experiments)	With the proposed scheme, mobile devices can achieve an optimum delay and also consume less energy with greater performance	We need to incorporate faster learning algorithms by considering problem-specific structures.
[54]	To Design a Smart Application capable of collecting the geo-tagged multimedia big data from different Hajj-related entities, the author came up with a framework that uses hybrid of clouds, one at the server end, and the other at crowd edge. A middle layer was added which serves as a proxy between the user end and the cloud infrastructure. When a user moves within a crowd, secure handshaking of metadata about the user is shared with the current edge node in order to share the current location.	Symmetric AES Encryption Algorithms	Prototype Implementation (Commercial Mobile device)	The proposed scheme supported context-aware services to millions of pilgrims that yearly gather together in a relatively small piece of land	More powerful nodes need to be employed. Also, there is a need to have more proper handshaking between the nodes and end-users.
[55]	The difficulty associated with privacy protection of wireless sensor location in edge computing is considered by the authors. Two privacy preserved location protocols; Trilateration and Multilateration, based on Pailliesr's homomorphic encryption system were employed. In order to obtain sensor location privacy, additional homomorphic encryption was applied. The two protocols with least-squares were selected and converted to privacy preserved protocol. Based on the applied homomorphism, the cipher text of the solution was computed by the cipher text of each distance.	Asymmetric Homomorphic Encryption	Mathematical Analysis	The proposed Scheme protects the privacy of the actual location information as compared to other schemes that protect location privacy by identity concealment.	Other wireless algorithms cannot be applied directly to the proposed scheme to generate their privacy preserved version.
[56]	To protect the network privacy of a mobile user with little impact on communication performance, the author proposed a novel differential location-based Privacy-Preserving framework deployed on the edge computing network. The designed techniques aimed at providing location privacy that balances between utility and privacy	Other method (MSS, i.e. Mobile Support System)	Simulation (Computer Simulation Experiments)	With the proposed scheme, the system operation cost is drastically reduced, and also the connection interruption for roaming mobile users' has also been eliminated	Need to device a means of hiding the user's network location as well as traffic from communication peers
[57]	The same authors as above devised a means of hiding the edge computing mobile users' network location and traffic from communication peers. The objective is to propose a distinct novel privacy-preserving location-based service usage framework that will be deployed on the edge node. A dynamic proxy network is developed for every mobile user in the network.	Other method (multiaccess edge)	Simulation (Computer Simulation Experiments)	The proposed technique provides flexible protection that balances the utility and privacy	Cost and performance need to be optimized
[58]	Considering the challenge that leads to leakage of users' location information through a side-channel, the authors propose the scheme by utilizing chaff services and considering heuristic strategies that mimic users' mobility to defend the users against eavesdropper tracking. They also design an optimized strategy to minimize tracking accuracy. The objective is to investigate a new side-channel that was not investigated before, and also to model an eavesdropper as a maximum likelihood detector.	Other method (Chaff Services, Heuristics and optimized strategies)	Simulation (Computer Simulation Experiments)	The proposed system significantly protect the user location privacy for users with highly predictable mobility	Need a defense against an advanced eavesdropper that can easily be aware of the optimized strategy
[59]	To propose a technique that utilize randomization against an advanced eavesdropper strategy awareness, the above similar authors improved their technique to protect the users against a more advanced eavesdropper, by introducing an extended strategy that utilizes randomization.	Other method (Chaff Services, Heuristics, and advanced optimized strategies)	Simulation (Computer Simulation Experiments), and Real Dataset	• The proposed technique can drastically reduce the tracking accuracy for users with highly predictable mobility. • The technique is capable of protecting end-users' location privacy even for highly predictable mobility users.	We need to consider cost and privacy tradeoff by replacing chaff with lesser cost services.

TABLE 5. ***(Continued.)*** **Summary of the privacy-preserving techniques.**

[60]	The scheme objectives are to locate missing people in a high-density environment where wireless infrastructures are limited, and also to deal with the challenge concerning real-time secured location services in a highly populated environment with millions of people. The authors proposed a panoptic system similar to the Amber alert system which executes computer vision algorithms to search for missing people. The technique aimed at locating missing people in a high-density environment characterized by limited wireless infrastructures.	Other method (Amber alert system, and D2D communication)	Prototype Implementation (Commercial Mobile device), and Real Dataset	Apart from ensuring users' location privacy, the proposed scheme can be used in lowering data through wireless infrastructures which will reduce batteries run down of mobile devices.	More powerful edge node need to be deployed (E.g. Deployment of fixed node cloudlet architecture)
[61]	The authors aimed at proposing a differential novel privacy-preserving Location-Based service usage framework that will be deployed on the edge node. The authors proposed a novel differential location-based privacy-preserving framework deployed on the edge node, in a view to solving the problem associated with poor quality of wireless sensor networks in providing massive and real-time data transmission. In the scheme, a service usage framework that is based on location privacy-preserving was proposed, which is used to protect individual privacy location.	Other method (Privacy Level Adjustment Module)	Prototype Implementation	The proposed technique provides flexible protection that balances utility and privacy.	More efficient ways of addressing the location and time-dependent cached data needs to be considered.
[62]	The objective is to eliminate the unexpected data disclosure risks at the edge node when traditional based query optimization technique is applied, and also to solve the problems associated with the unexpected data disclosure risk at the edge node when users' lodge a query so as to be able to select their favorite product in edge computing. The authors proposed a framework called Query-Guard that simultaneously tackles the problem associated with privacy distributed query processing issues and optimization of queries for latency.	Other method (Query processing pattern)	Prototype Implementation	Introducing a new privacy and latency awareness query optimization framework that tackle the problem associated with the traditional query-based optimization which increases the overall latency.	The query optimization mechanism needs to be improved in order to secure the privacy of other insensitive but important data.
[63]	The objectives of the scheme are to propose a supplementary algorithm for realizing optimal pairs of the probability and the privacy protection level, and also to produce an optimal solution to creating a channel assignment plan by employing applications on the network user side, with the aim of maintaining the privacy of data transmitted over less secure wireless sensor network. The authors came up with an approach that supports multichannel communication in edge computing. They utilized Dynamic Programming in generating an optimal solution. The proposed technique also considered the success likelihood of data transmission.	Other method (Dynamic Programming, Dynamic, MultiChannel Communication Model)	Simulation (SIM-DMC)	• The study vigorously supports multichannel communications on the edge of the thing, which can provide a higher level of privacy protection under timing constraints. • The study solved the problem that restricts the implementation of secured communications in a situation where data size becomes large by considering both connection probabilities and timing constraints.	• Problem with unpredictable inputs due to the fact that the employed dynamic programming uses only obvious inputs to produce expected optimal output • Dynamic programming is associated with high timing complexity. Thus, there is a need to investigate the methods for shortening the execution time.
[64]	The objectives of the study is to analyze the privacy conflicts of the computing tasks on the internet of connected vehicle, to design a V2V communication-based routing, and to adopt an algorithm that will realize multi-objective optimization in order to reduce the execution time and energy consumption of edge computing devices as well as privacy conflicts of computing tasks. The authors proposed an efficient computation offloading model called, ECO. Initially, privacy conflicts of the computing tasks on the internet of the vehicle are analyzed, followed by the design of a routing protocol for V2V communication for the vehicle. NSGA-II was utilized to achieve multi-objective optimization which reduces the execution time and prevents data and location privacy. The aim is to tackle the challenge associated with the risk of privacy leakage leading to tracking, identity tampering, and virtual vehicle hijacking caused by wireless communication during computation offloading in Mobile edge computing applications (Internet of a connected vehicle).	Other method (ECO, V2V Communication-Based Routing, and NSGA-II)	Simulation (CloudSim), and Real Dataset	Realization of multi-objective optimization that reduces the execution time of the computing tasks as well as energy consumption of the edge computing devices.	• There is a need to adapt and extend the proposed method to a real-world scenario of Internet of Vehicle services. • The various requirements of the computing tasks need to be specified to effectively identify an offloading strategy that will achieve energy savings of edge Computing devices

with the biometric fingerprint for wireless devices, hence improving the overall privacy of wireless communication. RF fingerprint is more reliable than the biometric fingerprint because it can be achieved with relatively low-cost receivers, which provide extra network security layers [48]. Most importantly, it can be used in identifying the sources of electromagnetic transmission, which make it the backbone of the security of a radio network for eliminating the known attacks [48]. Moreover, It is quite impossible to regenerate the fingerprint from any device whatsoever [49].

Fig. 11 illustrates the classification of the performance evaluation analysis methods employed by the studied techniques identified by the review work. They are classified into 2; methods with tools, which simply refer to the methods that employ software or hardware in the evaluation process, and methods without tools, which are the methods that did not employ software or hardware in the evaluation process. As shown in Fig. 11, the analysis techniques under analytical methods with tools include; Simulation (using MATLAB, NS3, NetLogo, PeerSIM, IFogSim, CloudSim, SIM-DMC, and Computer Simulation Experiments), prototype implementation (using either commercial mobile devices or embedded devices such as Single Board Computer, FPGA, and Microcontroller), Formal security Proof (Using ProVerif, and Scyther), Dataset (using both Synthetic and Real), Algorithmic proof (Game Theory), and Case-Study, whereas, Informal Security proof (using theorems and proofs), and, Mathematical analysis, are classified under analysis without tools.

2) EVALUATION METRICS EMPLOYED BY THE TECHNIQUES (DATA ANALYSIS TO ANSWER RQ4)

This section will review the evaluation metrics used in evaluating the performance of the techniques, with the intention of answering RQ4. According to the review work, the techniques employed different performance metrics to determine the intended aim. Table 11 summarizes the metrics employed by the respective technique with the corresponding purpose of using the metrics.

3) CLASSIFICATION OF ATTACKS ON EDGE COMPUTING NETWORK (DATA ANALYSIS TO ANSWER RQ5)

The attackers' aim on a network is to gain access and alter the vital information for fulfilling their needs or for selling purposes [105]. In this paper, edge computing network attacks are explored in an attempt to answer research question 5 (RQ5). Fig. 12 illustrates the taxonomy of edge computing

TABLE 6. Summary of the authenticity techniques.

REFERENCE	DESCRIPTION	TECHNOLOGY	PERFORMANCE ANALYSIS METHOD	ADVANTAGES	LIMITATION/GAP
[65]	To overcome the possible attacks associated with untrusted or malicious edge node and edge data centers of edge computing, the authors proposed a trustworthy scheme that takes into consideration both edge caching and bandwidth allocation for mobile users. The objectives are to design a trust evaluation mechanism to determine the security of each edge node, and to employ the reverse auction game to find the optimal edge node. A trust evaluation mechanism was designed to authenticate each edge node, employing direct trust and indirect trust. A reserve auction game is employed to assist the user to select an optimal edge node for content caching. Lastly, Bayesian Equilibrium acquired from the game analysis is employed in coming up with an ideal plan for the edge node.	Game theory Algorithm	Simulation (Computer Simulation Experiments)	Prevention of attack from untrusted edge nodes and improvement in the quality of mobile users experience	The scheme cannot prevent users' privacy disclosure when their information is cached on the edge node.
[66]	Concerning the challenge associated with secure information sharing and delivery among the different edge computing connected devices, the same author as above developed a reverse auction game to allow mobile users with optimal content caching of the edge node. A trust management method was designed to enable reliability evaluation of the selected edge node using direct trust evaluation. The objectives are to employ a reverse auction game for encouraging edge nodes to provide caching services, and to design a trust management method.	Game theory Algorithm	Simulation (Computer Simulation Experiments), and Algorithmic proof (Game Theory based)	The scheme provides a secure content delivery with less energy consumption. Also, delay and caching ratio were improved when compared with other similar schemes.	There is a need to consider the possibility of privacy disclosure by mobile users when their individual contents are cached on the edge nodes.
[67]	Addressing authentication problem of the in-home therapy application of mobile edge computing, the authors considered securing an in-home therapy. The author proposed an edge computing framework that enables secure and low latency diagnostic data sharing. A blockchain-Tor-based distribution transaction was employed for security purposes.	Block-chain Algorithm	Use case, Prototype Implementation	Supporting a large number of physically challenged patients at a considerably low processing time and under the secure condition.	Need to propose ways of storing both the immutable hashes of the therapy metadata and the actual multimedia location, in order to increase the level of authenticity.
[68]	The objective of the study is to overcome the possible attacks associated with untrusted or malicious edge node and edge data centres of edge computing. The authors proposed a technique that focus both on the identification of idle edge data centres (EDCs) for load balancing and authentication of the EDC. At the initial stage, each participating EDCs scrutinize each of the neighboring EDCs for authentication. This prevents malicious EDCs from interfering with the load balancing.	Load-Balancing Algorithm	Informal security proof, Formal security Proof (Scyther) Simulation (MATLAB), and Prototype Implementation (Single Board Computer)	Ensuring the authenticity of edge network interacting datacenters as well as balancing the load between them.	Lightweight security solutions need to be added to the proposed scheme for improving the security, efficiency, as well as load balancing performance and of edge datacenters.
[69]	The authors considered the possible attacks by untrusted or malicious edge node and edge data centres of edge computing. They proposed an integrated trust model based on comprehensive trust and evaluated the trustworthiness of the edge node. They constructed a framework for ensuring identity trust, behavioural trust, and ability trust of edge nodes. The activities of these edge nodes were coordinated and controlled.	Other Method (Integrated Trust)	Simulation (Computer Simulation Experiments)	With the proposed scheme, an efficient edge computing can be achieved based on comprehensive trust.	To achieve more efficient trust, a trust overlay network and global trust update method should be used instead of the trust measure and local trust update respectively.
[70]	The authors proposed an authentication scheme that considers both service providers' node and edge node. The objective of the study is to enable seeders-guard against malicious client nodes and also, to monitor and asses, the enabled seeders. The bit-torrent protocol is modified to form a test-bed using the Peersim simulator. A reputation bootstrapping mechanism was derived to ensure the reputation of each peer is accordingly bootstrapped. A method for enabling a service providers' node to access the reputation of each user node was also derived.	Other Method (Bit-Torrent Protocol)	Simulation (PeerSim)	Improve trust and network security in edge layers when compared to other similar schemes.	• The algorithm needs to be improved to fully cover other mobile edge-clouds use-cases. • There is a need to automate the determination of security level for different applications
[71]	To establish trust among the connected devices in the edge computing environment, the authors have adopted the idea of the Global trust degree of devices and proposed a lightweight trust mechanism based on multisource feedback information fusion. The scheme is reliable against bad-mouthing attacks generated from feedback providers. The objectives of the studies are to adopt a lightweight trust evaluation mechanism suitable for edge computing paradigm and to adopt a feedback information fusion algorithm based on objective information entropy theory which overcomes the limitation of the traditional trust scheme.	Other Method (Multisource feedback information fusion, information fusion algorithm, objective information entropy)	Simulation (Net-Logo)	Improve in computational efficiency and reliability when compared to existing approaches.	Trust management should be incorporated and improve into the proposed scheme to encourage cooperation between edge computing devices.
[72]	To propose a trust management framework that can evaluate trust for application and computing resources, and to apply the proposed trust management framework, the authors applied a derived trust management framework based on measurement theory, with trustworthiness and confidence as metrics. Traffic flows are used to obtain a device-to-device trust. For the trust value of tasks involved, they are configured to use the network element appropriately. However, when evaluating tasks' trustworthiness, both devices and flows were considered.	Other Method (Trust Management System (TMS))	Mathematical Analysis	Configuration of resources based on real-time trust information, ensuring both trustworthiness and confidence.	There is a need for security enhancement through the use of a better security algorithm, e.g. Lightweight security algorithm.
[73]	The objective of the scheme is to secure information sharing among the connected communication devices in a smart grid environment and to develop a secret key agreement protocol for the Smart Grid infrastructure. The authors deployed an identity-based signature as a key agreement protocol that allows smart meters to be connected to a utility control in order to collect the services they provided. The smart meters used the private key to connect the utility control in the absence of trusted authority.	Other Method (An identity-based signature, random oracle model)	Mathematical analysis, and formal security proof (ProVerif)	• The proposed scheme offered authentication and also smart meter unrecognition ability • It reduces communication overhead and delays by eliminating the role of a trusted authority.	There is a need to propose ways of reducing the computation cost.

TABLE 7. Summary of the attack detection techniques.

REFERENCE	DESCRIPTION	TECHNOLOGY	PERFORMANCE ANALYSIS METHOD	ADVANTAGES	LIMITATION/GAP
[74]	A cooperative defense framework against distributed denial of service attack (DDoS) for mobile edge computing is proposed by the authors. The scheme leveraged the network function and software-defined networking algorithms. The objectives are to design a framework on a cooperative defense framework against denial of service attacks, to design an appropriate utility by considering the resource usage efficiency, and to propose an online algorithm that has a performance guaranty. The edge nodes with less defense capability are supported by self-defense edge nodes. A multi-requester as well as multi-provider resource management issue was developed to balance between complexity and proposed scheme performance.	SDN Architectural Framework	Simulation (NS3)	The first scheme to explore cooperative defense against denial of service attacks in mobile edge computing.	More key techniques for detecting denial of service attacks need to be incorporated.
[75]	In an effort to detect the attacks that hinder the offloading mechanisms in edge computing applications, the authors studied an online security-aware edge computing under jamming attacks. The objectives of the studies are to develop an approach that will tackle security problems of edge computing based on MAB framework and to develop a SAVE-S algorithm modified form of stochastic jamming, for selecting the most convenient server with minimum security concern for offloading of computational tasks.	MAB Architectural Framework	Prototype Implementation, Real Dataset, and Synthetic Dataset	• Avoiding of Jamming attacks by selecting a reliable server for offloading of the computing tasks associated with minimal security concern without utilizing extra resources • The scheme ensures reliable and secure-offloading with minimal edge resource utilization.	The scheme needs to be improved to detect other attacks not only jamming attacks.
[76]	The objectives of the scheme are to focus on the detection of attacks of offloading in edge computing and to propose a secure vehicular edge computing network that will optimize the efficiency of task offloading in an attempt to prevent the network attacks from obstructing offloading operations. The authors devised a secure vehicular edge computing, a framework based on a behavioral game. Malicious edge nodes tend to disturb the offloading process by introducing attacks to the system. To prevent the execution of the attacks, they developed cooperative and uncooperative games. The vehicles, cyber defense center, and distributed security agent cooperate and ensure secure offloading, whereas the attackers undertake uncooperative approaches to introduce an attack by hacking the communication between authorized nodes.	Game Theory, Algorithm	Simulation (NS3)	Enhancing the detection and classification rate of malicious edge node, as well as optimizing the end-to-end delay of offloading tasks.	Smart and collaborative attacks of offloading operation need to be investigated.
[77]	The study aims at detecting attacks in the edge computing environment resulted due to the vulnerability, open features and distributed nature of the computing paradigm. The author proposed a scheme based on attribute attack graphs. The attack graph was developed with the use of a security alarm association and a false alarm determination network. A formal correlation analysis is performed on the contributing relation of the alarm information. A minimum dominance set solution of the attribute attach graph was generated by transforming linkage defend strategy decision computing. A set of attack linkage disposal decision-making technologies is then constructed from the designed linkage disposal strategy execution point decision algorithm based on a greedy algorithm.	Greedy algorithm	Prototype Implementation, and Real Dataset	The proposed scheme provides a timely and effective defense against attack	There is a need to automate the determination of the security level for different applications.
[78]	Considering the above similar challenge, the authors proposed a spoofing detection mechanism based on multiple channel attributes, with the aim of considering multiple channel attributes. The clustering algorithm is further deployed to enhance detection and to reduce technique complexity.	Clustering Algorithm	Simulation (MATLAB)	• Provision of optimal performance with significantly lower complexity • The technique has a better performance compared to single attribute detection	More experiments other than simulation needs to be carried out to evaluate the performance of the scheme.
[79]	To propose a distributed detection scheme, the authors developed an attack detection system by employing extreme Machine Learning (EML). The EML uses HPC cluster resources of the cloud on any trainer task that is characterized by time-consuming and high computation.	Machine Learning	Synthetic Dataset	• Achieved an efficient computation and analysis of the collected data in an edge computing network. • The scheme had better performance coupled with faster learning and training speed.	Edge nodes located far from the data source needs to be protected, apart from those very close.
[80]	An attempt was made by the authors to isolate a malicious edge node in edge computing. The objectives of the scheme are to propose a defense technique for D2D communication, to design classical honeypots to isolate attacks and to propose attack detection and tracking algorithms. Considering an environment in which a set of mobile devices perform the task of computational offloading, they proposed a defensive technique for Device to Device (D2D) communication, called HoneyBot. The tracking mechanism that handles insecure D2D infected communication channel was developed to track and isolate any malicious nodes.	Other Method (D2D Communication)	Prototype Implementation, and Real Dataset	• Performance evaluation is conducted in a real university network and proved to be helpful in detecting attacks of malicious node • The scheme detects tracks and isolates any malicious node.	Insider attacks need to be tracked and detected; hence a reliable tracking and detection mechanism needs to be employed.
[81]	The scheme is proposed with the objectives of exploring the limitations of current mobile malware detection techniques, to investigate the different feature extraction and detection techniques, and to develop malware detection techniques based on permission feature. The authors proposed a scheme that detects mobile malware which adapts to avoid detection. Behavioral analysis was developed to determine statistical analysis, dynamic analysis, and permission on when and how to determine the application logic behavior is yet to be executed.	Other Method (Hybrid feature analysis)	Real Dataset, and Prototype Implementation	The technique outperforms other mobile malware detection techniques.	The detection engine needs to be improved to ensure zero-day protection in detecting both known and unknown malware.
[82]	The authors proposed a scheme to detect spoofing attacks on GPS signals at the edge, and also reconstruct the attacked signal, with the objective of developing a validation mechanism for detecting GPS spoofing attacks on vehicles. The GPS signals at the edge node are collected and compared with the signal received from the satellite. Any difference with the GPS signal, reveal spoofing attack has occurred.	Other Method (GPS)	Real Dataset	• Low cost, sufficient, and accurate in detecting all simulated GPS spoofing attacks • The scheme can be used as a backup plan to eliminate the massive failure of GPS in navigation applications	There is a need to improve the scheme for detecting other attacks other than GPS spoofing attacks.
[83]	The authors proposed an approach named PANGUARD, for detecting a third-party library. The objectives of the scheme are to propose a novel combination of features in applications so as to characterize third-party library, to adopt Set Analysis in order to optimize third-party library detection and to implement the proposed technique and apply it in an industrial edge computing scenario. A combination of features containing both structural and content information is used to characterize third-party libraries. A set analysis that speeds up the detection are adopted.	Other Method (ANDROIDS)	Real Data Set, and Prototype Implementation	• High accuracy and scalability in detecting third-party library for Android Applications • The scheme is capable of real-time detection with both accuracy and scalability	There is a need to search for the optimal value of the child node which is not covered in the proposed technique.

TABLE 8. Summary of the authenticity and privacy-preservation techniques.

REFERENCE	DESCRIPTION	TECHNOLOGY	PERFORMANCE ANALYSIS METHOD	ADVANTAGES	LIMITATION/GAP
[84]	The authors proposed an identity authentication framework based on privacy-preserving face recognition. The aim is to design a framework for a privacy-preserving edge computing-based face recognition system for authenticating users. For extracting the face features, the convolutional neural network is employed. A method of nearest neighbor that computes the cosine similarity over encrypted features vector is used to overcome the problem of privacy leakage. In order to increase the fault tolerance features of the scheme, the technology of a secret sharing homomorphism is used.	Secret sharing Homomorphism mechanism	Synthetic Dataset, and Simulation (Computer Simulation Experiments)	With the employed secret sharing homomorphism, the fault-tolerance of the proposed scheme is enhanced.	The encryption algorithm needs to be improved to reduce the consumption time of the authentication process.
[85]	The authors try to maintain the tradeoff between authentication and privacy-preservation of IOT end-devices with weaker identity in an edge computing environment. The aim of the scheme is to propose an authentication protocol for end-user devices with weaker identity in order to achieve a tradeoff between privacy and authenticity. The proposed scheme uses a combination of short group signatures and Shamir's secret sharing scheme. Six different attacks were used in analyzing the security property of the scheme, which proved its feasibility.	Shamir's secret sharing mechanism	Prototype Implementation, and Formal Security proof (Proverif)	The authors achieved 4 goals that include Authenticity, Privacy-preservation, accountability, and dynamic removal.	There is a need to automate the determination of the security level for different applications.
[86]	The authors proposed a security framework that ensures privacy-preservation and authentication for big data multimedia content in an edge computing environment. The objectives of the scheme are to provide a secured multimedia content retrieval with the intention of eliminating malicious edge node and to prevent privacy breaches by trusted, but curious edge node and users. Each edge node is modeled as a distributed and context-aware learner. The various edge nodes communicate among themselves to understand end-users' preferences. Multimedia contents cluster tree is employed to handle the dynamically varying cached multimedia content dataset. The privacy-preserving is achieved with the use of a differentially private algorithm. To evaluate the trustworthiness of the authentication protocol, a trust evaluation mechanism is designed.	Algorithmic Method	Real Dataset	The scheme can provide support to the increasingly big datasets of multimedia, and at the same time maintaining a balance between privacy-preserving, trustworthy, and caching accuracy	An efficient way of addressing the location and time-dependent cached data need to be considered.
[87]	The authors proposed an ID-based group signature security mechanism. The objectives of the study are to propose a secret access authentication scheme with improved efficiency, to balance between security and efficiency in VANET, and to propose an efficient security scheme in vehicular ad hoc networks. In an effort to preserve the privacy of the vehicular node, multiple pseudonyms are employed. SVO logic is used to ensure the Scheme's security effectiveness.	Other Method (Multiple Pseudonyms, and SVO logic)	Mathematical Analysis	The secure authentication scheme is proved by SVO logic and found to be better in performance than other similar schemes.	New signature and encryption mechanisms need to be incorporated in order to provide more location privacy-preservation of the users.
[88]	To balance between efficient trust and privacy-preserving solutions in social-IoT, the authors proposed a scheme where crowd-sources are used as edge servers. An entropy modeling is used to achieve trust establishment among the computing devices. Fission managers that operate in the edge environment are involved in maintaining the privacy rules.	Other Method (Entropy modeling)	Synthetic Dataset, Informal Security Proof, and Case-Study	With the proposed scheme, trust is provided without authorizing an attacker to enter the network	There is a need to automate the determination of the security-level for different applications.

network attacks. The categories of the attacks with the corresponding existing counterpart measures with respect to edge computing infrastructures are given in the following sections.

C. MESSAGE ALTERATION ATTACK

In this type of attack, the eavesdropper manipulates the messages used by the legitimate edge computing entities. Attacks under message alteration category include:

1) INFERENCE ATTACK

The adversary analyzes the data transferred by the genuine edge network communicating unit to gain knowledge about the entities. In [55], the authors extracted location obfuscation sub-issue to solve the problem of inference attack, and derive a modeled that represent a privacy game issue and solved it according to the obfuscated locations. In another attempt of eliminating the inference attack, authors in [67] proposed a Query-Quard framework that avoids potential private information leakage to the third-party by generating privacy-preserving query plans.

2) COLLUSION ATTACK

The malicious entity combines together two or more copies of information communicated by the trusted edge nodes to produce a completely new copy. Authors in [59] solved the problem of collusion attack by encrypting the communicated messages with symmetric AES cryptographic protocol. At each instance of the communication process, new AES keys are used for encrypting the message involved. Authors in [75] solved the problem of collusion attack by adopting a neighbor similarity method. When an edge entity requests for recommendations, they also incorporate a request for randomly selected trusted neighbor which is entirely different from the neighbor being inquired.

3) REPLAY ATTACK

The third-party intercept the information sent by the genuine edge entity and transmit it to another legitimate edge entity as if it is from the original sender. A key agreement protocol is utilized by authors in [78] for solving the replay attack problem in smart grid edge computing infrastructure. A single private key is utilized by smart meters for obtaining services from the utility control center. In [92], the authors deal with a replay attack by incorporating a timestamp to the signed message used for authenticating the communication between the edge entities. Similarly, in [97] and [95], the authors use a timestamp to prevent the replay attack. In [90], a timestamp together with Shamir's secret sharing algorithm is used in

TABLE 9. Summary of the techniques that considered more than two security/privacy requirements.

REFE-RENCE	DESCRIPTION	TECHNOLOGY	PERFORMANCE ANALYSIS METHOD	ADVANTAGES	LIMITATION/GAP
[89]	The authors proposed a security technique that considers privacy-preserving, authenticity, and integrity requirements in a mobile computing network. Three participating devices in the mobile edge computing network that include: end-user devices, edge servers, and public cloud center were assumed by the authors to design a privacy-preserving data aggregation scheme for mobile edge computing. The data from the end-devices are encrypted before transferring to the edge server. The edge server then sums all the received encrypted data and transferred to the cloud server. The public cloud center then decrypts the data using its private key for further action.	Cryptographic	Simulation (NS3), and Mathematical Analysis	Apart from ensuring data privacy, the scheme ensures authentication and integrity, as well as saving almost half of the communication cost.	The experiment conducted for evaluation of the scheme is not enough, thus more experiments need to be carried out in the future
[90]	To design a lightweight privacy-preserving aggregation scheme that will balance between security/privacy requirements and online computational cost of an edge computing network, the authors proposed a lightweight scheme called LPDA-EC, which handle privacy-preservation, authentication, confidentiality, and integrity security requirements, as well as online computational cost in an edge computing network. The scheme employed online/offline signature techniques. It ensures data integrity under Diffie-Helmen assumptions.	Cryptographic	Simulation (Computer Simulation Experiments), and Informal Security Proof	Apart from ensuring lightweight security, the proposed scheme provides lightweight computational costs and communication overheads.	The scheme needs to be applied to specific scenarios
[91]	To propose a scheme that can maintain the tradeoff between good performance and security in edge computing network, the authors proposed a security model called MOM4cloud architectural model that extends the existing message-oriented middleware (MOM) of cloud security alliance (CSA). The aim of MOM4cloud is to incorporate more security requirements that include: confidentiality, integrity, authenticity, and nonrepudiation.	None- Cryptographic	Simulation (Computer Simulation Experiments) and Prototype Implementation	The scheme can serve as a reference to software architects who want to ensure their edge/cloud systems correspond with CSA rules and regulations.	There is a need to automate the determination of security level for different applications.
[92]	To design a scheme that ensures the tradeoff between security and efficiency for mobile user devices in a mobile edge computing network, the authors proposed a security scheme that ensures authentication, confidentiality, and integrity requirements in mobile edge computing network. It also enhances mobility support for IOT devices in the network.	None- Cryptographic	Simulation (Cloud-Sim)	Apart from maintaining the tradeoff between security and efficiency, the scheme also addresses the mobility problems.	Lightweight security solutions needs to be added to the proposed scheme to improve security.

preventing a replay attack. Likewise, authors in [106] solve the replay attack problem by adding a nonce to each message before sending it to the communicating entity.

4) CIPHER-TEXT ONLY ATTACK

The advisory used the number of encrypted messages to recover as many plaintexts as possible or even the secret key. Authors in [94] solve the problem of cipher-text-only attack by encrypting the data before sending it to the edge server. The edge server then aggregates and sends it to the public cloud center where it can be recovered using the cloud center's private key.

5) EAVESDROPPING/SNIFFING/SNOOPING ATTACK

The malicious party steals the information communicated by the genuine edge computing entities. In an attempt to overcome the eavesdropping attack, authors in [59] encrypted the smartphone data with asymmetric AES algorithm prior to the communication stage. In [106], the authors ensure that the transmitted data after the realization of the connection between edge entities and edge server is first of all encrypted with a session key known to the communicating entities. Similarly, in [103], the authors prevent the snooping attack by employing an authentication service that authenticates the entity receiving the output data. Additionally, a confidentiality service is employed to encrypt the output data for protection against the snooping attack.

D. NETWORK DISRUPTION ATTACK

Here, the attacker develops a mechanism for counterfeiting network resources to access the communication between genuine entities. The various attacks under this category include:

1) DENIAL-OF-SERVICE ATTACK

The malicious entity makes network resources unavailable to the genuine entities by interrupting the normal activities of the entities. In an attempt to solve the problem, authors in [76] reduce the dependency of the edge communicating entities on a cloud datacenter, which consequently removes the single point of failure in the entire edge infrastructure. Similarly, authors in [93] eliminate the dependency on the centralized servers by employing scalable and distributed systems that use end-user devices as mini-edge servers. In another attempt, authors in [85] proposed a honeypot, a defense technique against denial of service attack. It is capable of detecting, tracking, and isolating attack. Authors in [79] proposed a cooperative framework against denial of service attack by utilizing network function visualization and SDN (Software Defined Network) architecture.

2) JAMMING ATTACK

The malicious entity blocks the communication between the edge devices and the edge server. In an attempt to solve the problem, authors in [80] proposed a novel SAVE-S algorithm

TABLE 10. Summary of the techniques that did not consider any of the proposed requirements.

REFERENCES	DESCRIPTION	TECHNOLOGY	PERFORMANCE ANALYSIS METHOD	ADVANTAGES	LIMITATION/GAP
[93]	The authors proposed a scheme that prevents attacks in edge-computing internet of vehicles (EC-IoT). The scheme works based on generating dummy traffic delivery. To propose an attack prevention scheme in the network, the vehicles in the network are allowed to send dummy packets on to the trusted and identified roadside units, with the intention of misleading the traffic statistics which aimed at protecting the hotspot roadside units. The incentive mechanism is designed using a Stackelberg game approach.	Game Theory	Informal Security Proof, and Mathematical Analysis	The scheme effectively secures the EC-IOT network against roadside unit hotspot attacks.	There is a need to include approaches that will protect the entire roadside units, not only the selected ones.
[94]	The authors proposed a system that manages various security functions. Security proxy was incorporated to have a match with the network inherited security functions. A fuzzy interface system mechanism was deployed to develop a scheme that will manage the various real-time changing security functions in the mobile edge computing network.	Fuzzy Method	Prototype Implementation, and Mathematical Analysis	When compared to other similar techniques, there is an improvement in performance in terms of execution time and Inverted Generational Distance values.	There is a need to automate the determination of the security level for different applications.
[95]	The aim of the study is to propose a security scheme that will eliminate the single point of failure problem associated with the traditional security solution of VANET. The authors proposed a block-chain based secure scheme for the vehicular ad-hoc network. The scheme employed three-layer architecture including perception, service, and edge computing layers. The perception layer ensures security for the data transmitted through the block-chain paradigm. The service layer combines both the traditional cloud storage and block-chain for establishing data security. The edge computing layer, on the other hand, supplies computing resources and edge cloud services to the perception layer.	Block-chain	Did not evaluate their scheme	The scheme ensures that data are tamper-resistance and traceable through the use of block chain technology.	Performance evaluation of the scheme needs to be conducted to verify the effectiveness of the employed methods.
[96]	A scheme that managed security, privacy, as well as the service quality of an integrated clinical environment was proposed by the authors. The scheme allows resource allocation management of the network to be done at the network edge. This resulted in low latency and very high quality of service. The technique deployed NFV and SDN architectural framework to ensure high scalability, efficiency, and real-time communication of the integrated clinical environment.	SDN and NFV Architectural Framework	Simulation (Computer Simulation Experiments) and Prototype Implementation	The proposed scheme solves the problem of availability, scalability, efficiency, and communication management associated with a typical Integrated Clinical Environment.	The host network levels of the proposed architecture need to be implemented and validated effectively.
[97]	To propose a security and deadline awareness scheduling policing scheme in an edge computing network, the authors proposed a scheme called RT-SANE (Real-Time Security-Aware Scheduling on the Network edge). Application with priority privacy requirements is sent to the edge data centers. To attain performance and security, a distributed orchestration architecture and protocol is incorporated in the scheme.	Architectural Framework	Simulation (IFogSim)	The scheme ensures application privacy while achieving improves real-time performance.	More complex workflow need to be employed in the model.
[98]	The aim of the study is to propose a secure and energy-efficient computation offloading scheme for service workflows in mobile edge computing. The authors proposed a scheme that ensures security against attacks during the computation offloading process. A cryptographic security overhead model is designed to calculate the execution time of the security services, and then a computational offloading problem is formulated.	Cryptography	Simulation (Computer Simulation Experiments)	The scheme decreases the energy consumption of the mobile device and at the same time satisfying deadline and risk rate constraints.	We need to consider other security issues where workflow applications can be offloaded.
[99]	To propose a reputation management scheme that will ensure security and improve the efficiency of the vehicular edge computing network, the authors proposed a reputation management scheme called DREAMS (Distributed Reputation Management System) for improving security and network efficiency of vehicular edge computing. The vehicular edge servers are used for realizing local reputation management of tasks for the connected vehicles. A multi-weighted subjective logic is employed for updating the reputation in the system.	Other Method (Multi-weighted logic)	Simulation (Computer Simulation Experiments), and Mathematical Analysis	The scheme optimizes the behavior detection by recognizing the misbehaving vehicles.	Existing methods, e.g. Kullback-Leibler Distance can be used to improve the proposed scheme.

to secure the offloading of computational tasks. They execute the algorithm without utilizing extra resources.

3) BANDWIDTH ATTACK

The attacker transmits a large number of malicious packets to the edge network with the intention of overpowering its bandwidth. In [75], the bandwidth attack is dealt with using a trust and reputation-based approach. The edge nodes are enabled to guard against suspicious client nodes by monitoring and assessing their contribution to fellow client nodes.

4) FAKE-BLOCK ATTACK

The malicious entity sends fake files to respond to a download request from a legitimate edge node with the intention of wasting the download bandwidth involved.

5) SYBIL AATTACK

The attacker takes over a quite number of edge nodes in a network that lacks central management, which consequently hijacks the network. In an attempt to deal with the Sybil attack, authors in [75] employed the bootstrapping method to prevent attackers from joining the network. Similarly, in [93] the authors avoid threshold sharing with the requesting node and take a decision on a safe entity only.

E. CAMOUFLAGING ATTACK

In this type of attack, the adversary manipulates to penetrate the edge network as a genuine entity. Attacks under this category include:

1) IMPERSONATION ATTACK

The malicious party adopts the identity of the legitimate user to authenticate itself to the network. To dealt with impersonation attacks, authors in [59] encrypted the payload data with AES symmetric key algorithm. Moreover, the end-to-end signaling protocol is also inspired and followed accordingly. In another attempt, authors in [73] employed the AES algorithm to authenticate the legitimate edge nodes. A cloud shared key is used to encrypt the initial authentication packet followed by individual associated keys of the edge nodes. In [92], a Carbon Copy (CC) signature which is an identity-based signature is employed by the legitimate edge nodes during the authentication process. Elliptic curve cryptography is employed, where both the public and private keys are calculated by the trust authority.

2) MAN-IN-THE-MIDDLE ATTACK

The attacker secretly manipulates the communication between two eligible parties who believed they are directly communicating with each other. In [90], the authors used a shared symmetric key to encrypt the critical instruction at the

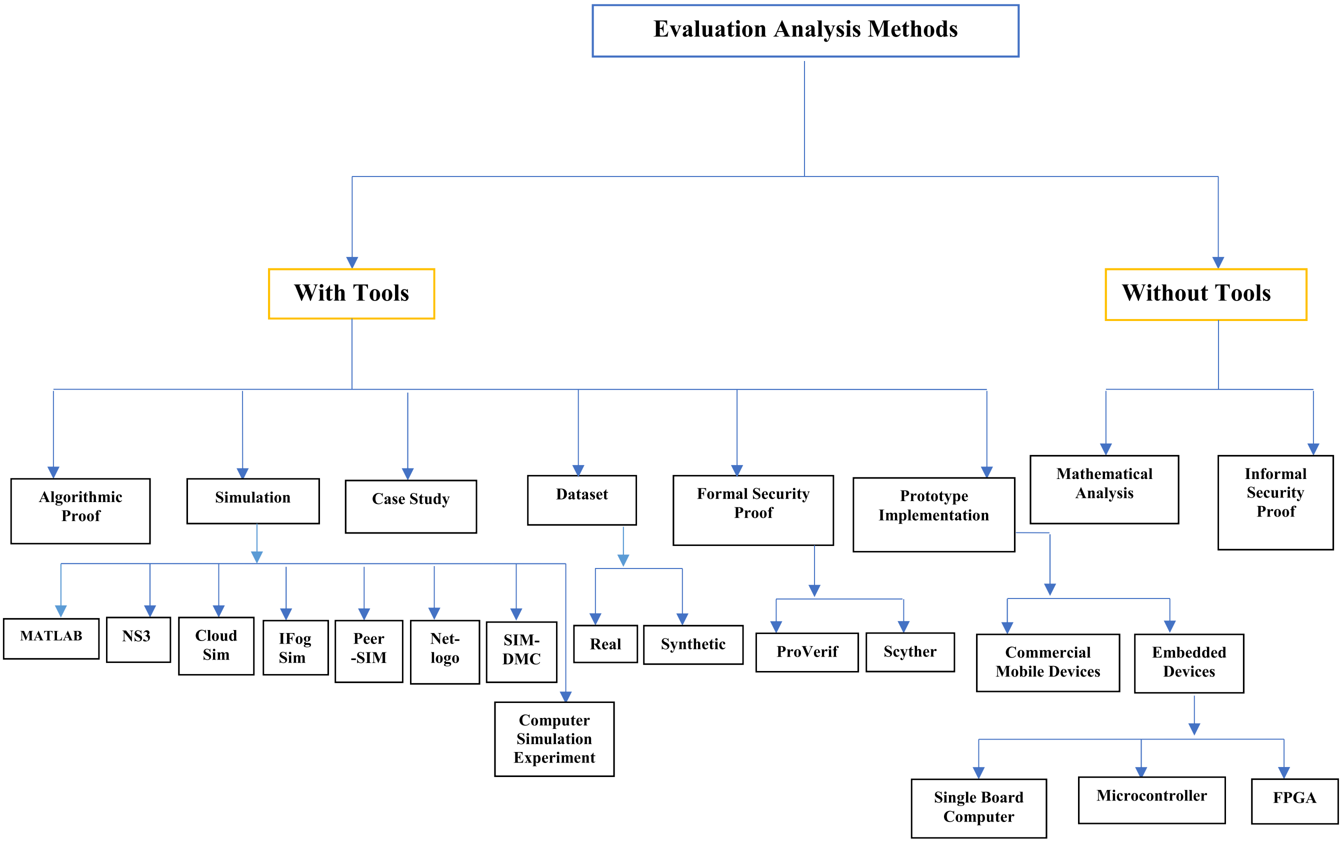

FIGURE 11. The classification of the performance analysis methods.

end-user device and edge device communication site. Hence, the attacker cannot construct a valid cipher-text without the symmetric key. Whereas, at the edge device and control center communication site, a group public key signature is employed for authenticating the identities of the group entities as well as the critical instruction. Therefore, the attacker cannot convince the control center to accept the forged group public key. Similarly, in [106], the session key cannot be deduced by the attacker because both the secret master key of the registration authority and free shared key are kept secret. In [45], a mutual trust mechanism is established in the edge network by employing lightweight encryption of the signal layer according to the access request sent by the wireless devices. Whereas, In [97],time stamps and encryptions algorithms are used to solve the man-in-the-middle attack.

3) ADDRESS RESOLUTION PROTOCOL (ARP) SPOOF ATTACK

In this type of attack, the malicious party links Media Access Control (MAC) address with the IP address of the legitimate edge devices, by sending false ARP messages across the edge network. Hence, the adversary camouflages with legitimate edge devices and harm the entire system. In [107], an ARP prefix processor, which is a form of SNORT intrusion detection system is designed to solve the problem of the ARP spoof attack. It generates alert whenever an ARP spoof attack is suspected.

F. PHYSICAL ATTACK

The adversary steals the physical components of the edge computing network and injects malicious data with the intention of harming the legitimate entities or the entire network. The type of attacks under this category include:

1) SIDE-CHANNEL ATTACK

The third-party compromised the functionality of a given cryptosystem by exploiting the physical edge computing devices. Authors in [53] prevented the employed AES cryptographic algorithm against the side-channel attack by random masking and shuffling of the S-BOXES. An attack detection technique based on distributed extreme machine learning technology is employed in [84] to eliminate the side-channel attack on the used cryptosystem.

2) SPOOFING ATTACK

The attacker impersonates the physical devices of the legitimate users to propagate malicious effect, steal data, or interfere with edge network access control. In an attempt to solve a spoofing attack, Yoon in [108] ensures that each participating sensor device transmits their data to a legitimate edge node in

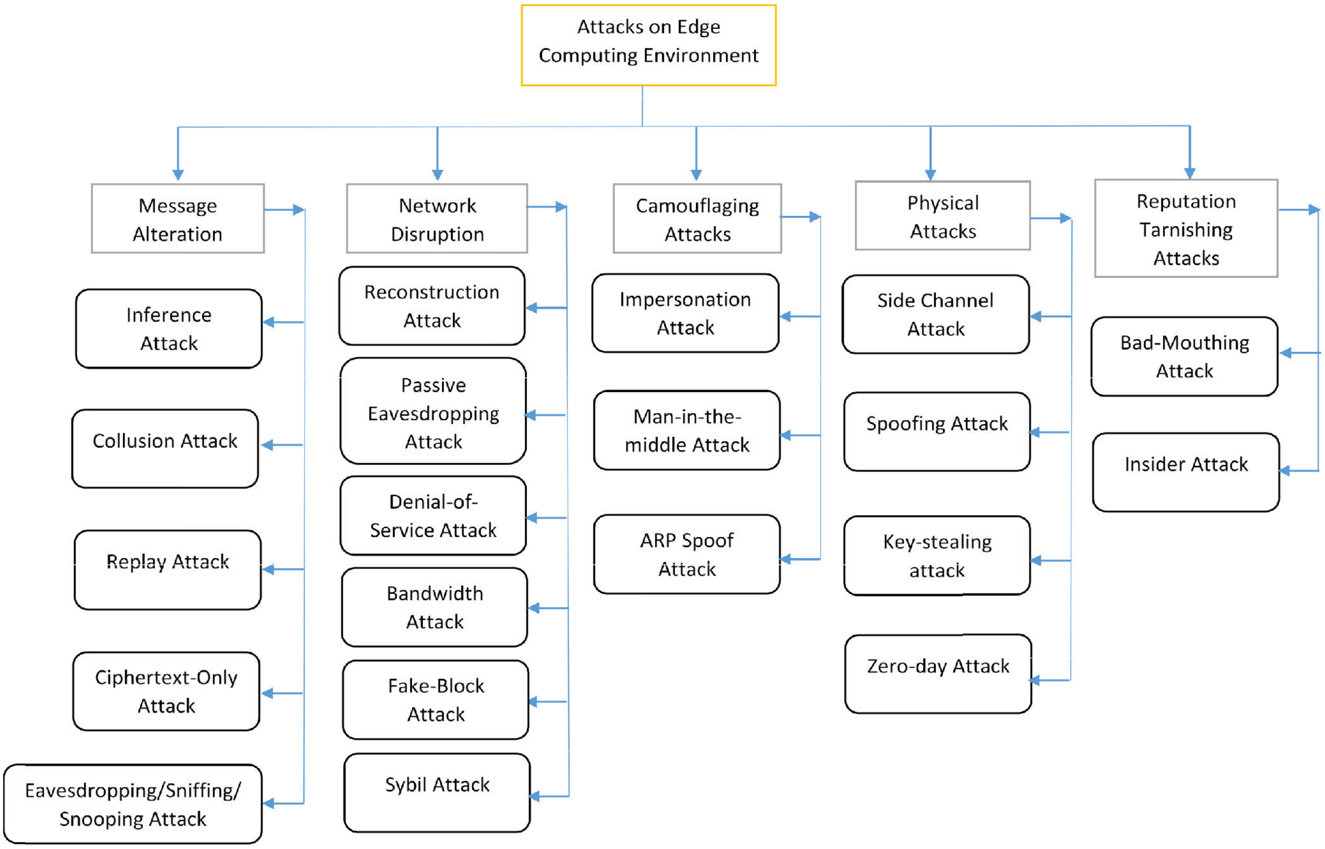

FIGURE 12. The taxonomy of the attacks affecting edge computing network.

the Java-Script Object Notation (JSON) format. The wireless sensor networks (WSNs) are requested to send the JSON data about their neighboring sensors. These are used to check the integrity of the data from the dynamically moving sensors. In another attempt to eliminate spoofing attack, authors in [87] devised a means of collecting information at the edge nodes and use it to cross-check the validity of the GPS signals received from the satellite. If the received signal is not genuine, the original GPS signal is reconstructed back. In [83], a spoofing detecting technique is devised using an improved heuristic clustering algorithm. The edge server is made to report its real-time security condition to the cloud server for immediate countermeasures from any spoofing attack.

3) KEY-STEALING ATTACK

The intruder snatches the keys of the legitimate edge users to intrude on their communication. In [92], the authors proposed a means of eliminating the key-stealing attack by ensuring that the trust agent issues the keys to the legitimate edge users through a secure channel. Also, the group signing keys and the corresponding identities of the users, together with the shared key is encrypted by the roadside unit. Finally, the unit stores the private keys and shared keys in temper prove device.

4) ZERO-DAY ATTACK

The adversary utilizes the advantage of the weaknesses that exist in the physical resources of an edge network before they are discovered by the party responsible for the mitigation exercise. In [108], the authors used an artificial neural network to solve the zero-day attack problems. The tolerance and trigger areas constructed at a training stage are dedicated to ensuring the trustworthiness of the sensors.

G. REPUTATION TARNISHING ATTACK

The intruder frame-up negative feedback or dishonest recommendations for genuine entities with the aim of ruining their reputation. Attacks under this category include:

1) BAD-MOUTHING ATTACK

The attacker provides dishonest feedback to frame-up genuine edge users. In an attempt to deal with the bad-mouthing attack, authors in [109] developed a lightweight trust mechanism based on multisource feedback information fusion. The same authors in [76] incorporated objective information entropy theory-based feedback information fusion algorithm to solve the problems associated with the traditional trust schemes.

2) INSIDER ATTACK

In this type of attack, the adversary has authorized network access. By being a genuine entity of the edge network. Therefore, the adversary utilizes this advantage and harm other legitimate edge network entities. Authors in [85] proposed a honey-Bot mechanism that acts as a defense against edge network insider attack. The technique is capable of detecting, tracking, and isolating the malicious edge nodes that can cause an insider attack.

VI. DISCUSSION

Although the previous review studies have laid a noticeable foundation that helps in understanding the security and privacy issues in edge computing, however, many of the reviews have the limitation of not providing a thorough investigation of the security/privacy requirements. Additionally, the techniques for ensuring the requirements with the employed technological methods were also not fully explored. This review work adopted a systematic procedure that helps in providing a proper understanding of security and privacy in the edge computing environment.

Six research questions (RQ1 to RQ6) were formulated and thoroughly answered to achieve the targeted aim. With regard to RQ1, eight main security and privacy requirements were identified from the reviewed studies. Similarly, it can be observed from the outcomes of RQ2 that, out of the reviewed studies, 16 techniques were proposed under the Privacy-Preserving requirement, which is the highest number, when compared with the remaining requirements. This shows that a lot of research interest is given to this requirement. The next requirement that received interest is Attack Detection, with 10 proposed techniques, followed by Authenticity with nine, then Confidentiality with four. Only one technique considered the Availability requirement. Therefore, future researchers should consider this requirement. Six proposed techniques considered a combination of two different requirements. Moreover, four techniques considered a combination of more than two requirements. Fig. 13 illustrates the distribution of the techniques with respect to the requirements considered.

According to the review work, it can be observed that there is no technique that considers Integrity, Nonrepudiation, and Reliability requirements separately, except together with other requirements. This indicates that these requirements were not given much interest. Hence, future research should also concentrate on these requirements.

Besides, regarding RQ3, the identified techniques were further classified according to the employed technological methods. It can be seen that Paillier's Homomorphic Encryption, AES Cryptographic Algorithm, ABE Policy-Hidden, and Reverse Auction Game are the most commonly employed technologies. Also, with regards to the employed performance analysis methods, the dataset is most frequent when considering the analysis with tools. 11 studies employed a real dataset, whereas 4 studies employed synthetic datasets. The computer simulation experiment is the second most frequently used method. The most frequent simulation tool was NS3. In terms of the prototype implementation, an embedded device (Single Board Computer) is the most frequently employed device. The most frequent formal security analysis tool is Proverif, whereas the Scyther tool is employed by only one study. On the other hand, Informal security analysis is the most frequent method when considering methods without tools.

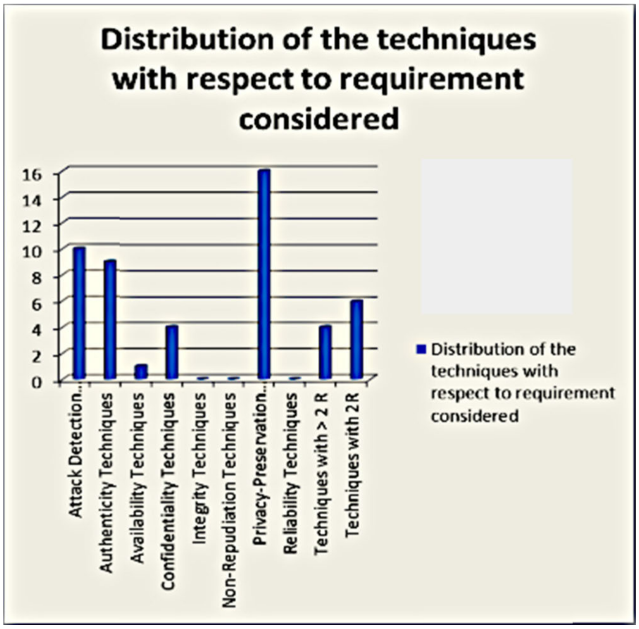

FIGURE 13. **Distribution of the techniques with respect to the requirements considered.**

The performance metrics employed in evaluating the effectiveness of the techniques were explored as specified by RQ4. It can be observed that the techniques under each class of requirement employed specific metrics in evaluating their performance, which verifies the intended aim. The purpose of evaluating the techniques with a particular metric is highlighted in Table 11. This will help future researchers in knowing the purpose of employing each metric under certain techniques.

With regard to the research question 5 (Q5), that emphasizes on the categories of attacks in an edge computing network, a taxonomy of the attacks is given in Fig. 12. Additionally, the trends of the technologies employed in curbing the attacks are also highlighted. Lastly, with regard to RQ6 that focuses on the research opportunities for future researchers working in the area of security and privacy in edge computing, the limitations of each technique are given in Table 4 to Table 10. This will help future researchers working in this area with forthcoming research gaps.

A. THREATS TO VALIDITY

The study focused on conducting the review work as well as possible. However, some factors encountered may change

TABLE 11. The summary of evaluation metrics employed by the techniques.

REFERENCE	REQUIREMENT UNDER CONSIDERATION	PURPOSE FOR THE EVALUATION	EVALUATION METRICS
[58], [59], [61]	Location Privacy-Preserving	To minimize detection or tracking of the user by the eavesdropper, and to achieve fine-grain security property	Tracking Accuracy
[60]	Location Privacy-Preserving	To minimize the energy usage of mobile devices	Energy Consumption
[56], [57]	Location Privacy-Preserving	Protecting mobile user's network privacy with reasonable effect on the communication performance	Performance Overhead
[56]	Location Privacy-Preserving	Protecting mobile user's network privacy with reduced operational cost	Operation Cost
[49], [60], [62]	Location and Data Privacy-Preserving	To lower data transfer with reasonable privacy protection	Execution Time
[54], [68]	Location Privacy-Preserving, Authenticity based Load Balancing	To ensure proper handshaking between end-devices and edge nodes	Response Time
[61]	Location Privacy-Preserving	To utilize edge nodes in providing real-time services	Service Quality
[50], [61], [63]	Location and Data Privacy-Preserving	Ensuring privacy protection that will prevent the third-party from accessing user's data, thus achieving fine-grain security property	Privacy protection level
[49]	Data Privacy-Preserving	To determine the amount of information an intruder will obtain after an attack in the edge network, and to achieve fine-grain security property	Mutual Information
[50]	Data Privacy-Preserving	To ensure privacy in an edge network where the precise location of users is required for task allocation	Task Acceptance Rate
[45], [46], [48]	Confidentiality	To reduce the overall time required by data user in edge computing to decrypt the cipher-text	Computation Time
[46], [73]	Confidentiality, Authenticity	To evaluate the lightweight property	Computation Cost
[46], [73]	Confidentiality, Authenticity	To evaluate the lightweight property	Communication Cost
[47]	Confidentiality	To evaluate the level of imperceptibility and distortion of watermarked images	Peak Signal to Noise Ratio/Structural Similarity
[48]	Confidentiality	To improve the collision attack on block ciphers	Success Rate
[71]	Authenticity	To evaluate the computational efficiency	Global Convergence Time
[71]	Authenticity, and Reliability	To evaluates the reliability of the trust computing devices	Task Failure Ratio
[65], [66]	Authenticity	To evaluate the contents data size that are cached by the authorized edge nodes to the total contents data size during the simulation process	Secure Caching Ratio
[65], [66]	Authenticity	To evaluate the average reduced repossess delay of the content of genuine edge nodes, compared to require contents from distant content servers	Average Saved Time
[69]	Authenticity	To evaluate the users' behavior in the edge network	Dynamic Adaptability
[67]	Authenticity	To evaluate the overall total delay in the dynamic computing system	Mean Processing Time
[79], [81]	Attack Detection	To evaluate the probability of identifying none-malicious devices accurately	True Positive Rate
[79], [80], [81]	Attack Detection	To evaluate the probability of identifying malicious devices accurately	False Positive Rate
[79]	Attack Detection	To evaluate the probability of identifying none-malicious devices wrongly	True Negative Rate
[79]	Attack Detection	To evaluate the probability of identifying malicious devices wrongly	False Negative Rate
[79], [81]	Attack Detection	To evaluate the number of the correct results with respect to all the returned results	Precision
[81]	Attack Detection	To evaluate the number of correct results obtained with respect to the number of results that ought to be returned	Recall
[79], [81]	Attack Detection	To evaluate the harmonic mean of Precision and Recall	F-Measure
[79], [80], [81]	Attack Detection	To evaluate the percentage of accurately identified devices	Accuracy
[79], [82]	Attack Detection	To evaluate error occurrence in detecting attacks in an edge network	Error Rate
[79]	Attack Detection	To evaluate the correlation between values that express a good level of agreement between prediction and observation	Mattew's Correlation
[76]	Attack Detection	To evaluate the mean-time taken by data to reach a targeted destination	End-to-End Delay
[77]	Attack Detection	To evaluate the defense effectiveness of a typical attack linkage disposal strategy	Intrusion Success Probability
[77]	Attack Detection	To evaluate the effectiveness of the generated attacks	Intrusion Time Test
[80]	Attack Detection	To the total number of messages introduced to the edge network from beginning till when the suspected node is identified	Overhead

the conclusion drawn, which may affect the quality of the findings. Below are some of the factors:

1) The data acquisition process is subjected to a biased opinion because only one author searched for the primary study articles.
2) Only four electronic databases were explored for collecting applicable data. Thus, relevant studies from other databases may not be included. This limited the scope of the review work.
3) Only journal articles and conference proceedings were included, whereas some other studies that may help

with additional information, such as patents, magazines, and symposium, were excluded.

VII. OPEN RESEARCH ISSUES

In this section, the research open issues in the field of security and privacy of edge computing paradigm will be given. The aim is to provide opportunities for future researchers willing to contribute to this area. The major open issues include:

A. LIGHTWEIGHT SECURITY FEATURES

Lightweight security is required in the edge computing network because of the minimum resource and storage characterized by the edge devices. The conventional cryptographic protocols are characterized with very high computation and communication costs [110], [111], due to the large key size employed. Therefore, such protocols cannot be applied directly to the edge network. As such, lightweight cryptographic protocols with smaller encryption keys that require fewer memory and CPU resources are preferred in edge computing. Lightweight security does not maintain the tradeoff between efficiency and security/privacy, as considered by most of the reviewed techniques. For lightweight security, efficiency is not as important as security/privacy.

It can be observed that most of the techniques under Confidentiality and Authenticity are not lightweight, that was the reason why they did not evaluate the techniques using the lightweight evaluation metrics (i.e. computation and communication costs). Only four techniques [50], [51], [53], and [78] employed the lightweight metrics. Hence, future research on security and privacy in edge computing should focus on lightweight security, for example, Elliptic Curve Cryptography, Permutation Based Lightweight Cryptography, Block-Ciphers Lightweight Cryptography, etc.

B. FINE-GRAIN SECURITY FEATURES

To attain fine-grain security features, a dynamic auto-update function needs to be incorporated into the privacy-preserving mechanisms, as well as an efficient data-sharing mechanism, due to the huge amount of data produced at the edge of the network by end-devices. The most commonly fine grain security evaluation metrics as depicted in Table 11 are Tracking Accuracy, and Privacy protection level, which were employed by only five techniques [55], [63], [64], [66], [68]. Therefore, future research should consider fine-grain features when proposing Privacy-Preserving techniques.

C. PRIOR INVESTIGATION OF ATTACKS

In most of the reviewed studies, attacks were not fully investigated and dealt with sufficiently prior to the design process of the techniques, especially the authentication and privacy-preserving schemes. These attacks are very dangerous to the privacy of the interacting edge devices, which may lead to revealing devices' secret information.

D. MORE WORK IS REQUIRED UNDER CERTAIN SECURITY/PRIVACY REQUIREMENTS

As stated earlier, some of the security and privacy requirements are either not having techniques that consider them separately, or not having at all. For example, from the findings, the Availability requirement is having only 1 technique under it, whereas Reliability, Nonrepudiation, and Integrity requirements are not considered by any technique, except in combination with other requirements. Due to the importance of these requirements, future researchers should concentrate on devising techniques that will consider them.

E. SECURE TWO-WAY COMMUNICATION

The establishment of secure two-way communication in the edge network is relatively difficult compared to the cloud network with ready-made security mechanisms. Therefore, to achieve secure two-way communication in an edge computing network, lightweight key exchange algorithms that suite edge computing should be designed in the future.

F. PROPER UTILIZATION OF INTRUSION DETECTION MECHANISMS

Intrusion Detection Systems (IDS) are employed for detecting and mitigating of the various attacks in a network. However, in an edge computing environment, the IDS need to be applied to the various layers of the edge network (Edge nodes, end-users, and, cloud). Applying IDS to only one or two layers may not guarantee that attacks from the malicious party will not propagate to the entire edge network.

G. UTILIZATION OF PROGRAM (SOFTWARE) ANALYTICAL TOOLS

The security and privacy issues in edge computing network are diverse. Consequently, utilization of software-based security and privacy analysis will help in quick and efficient identification of such issues. The scope of these software analysis in edge computing is still an open issue for future research.

VIII. CONCLUSION

Edge computing is a promising paradigm aimed at eliminating almost all the drawbacks associated with cloud computing. Security and privacy issues are among the significant challenges affecting its acceptance. As such, studying ways of mitigating the problems is of paramount importance. Findings show that the devised systematic literature review is the first of its kind in edge computing security and privacy perspectives. It aimed at providing a comprehensive and reflective understanding of the security and privacy requirements, the state of the art techniques for ensuring the requirements, as well as the technological methods employed by the techniques. With this in mind, a total of 78 articles were thoroughly studied, in line with the standard SLR procedures. After a thorough analysis of the extracted data, the findings reveal essential results. Firstly, the taxonomy of security and privacy requirements was derived. The study found that there are eight classes of requirements as far as edge computing security and privacy is concerned. Secondly, the study discovered that each requirement has its specific techniques designed mainly for it, except integrity, nonrepudiation, and reliability which were considered together with other requirements in four different identified schemes. Thirdly, the findings classified the identified techniques under their corresponding technological methods employed with the aim of identifying the trend. Fourthly, the review work has identified limitation of each of the techniques which lead to research opportunities for future researchers to concentrate on. Moreover, the attacks affecting the edge computing network have been thoroughly explored. The taxonomy of the attacks as well as the employed technological methods for their elimination have been revealed. Moreover, it was observed that each category of the techniques under a particular requirement has specific metrics used for evaluating its performance for ensuring certain aim. Lastly, future research open issues were included for the benefit of researchers willing to work in the area of edge computing security and privacy.

ACKNOWLEDGMENT

Authors of this research are thankful to the reviewers for their observations, comments, and recommendations to enhance manuscript contents.

REFERENCES

[1] H. El-Sayed, S. Sankar, M. Prasad, D. Puthal, A. Gupta, M. Mohanty, and C.-T. Lin, "Edge of things: The big picture on the integration of edge, IoT and the cloud in a distributed computing environment," *IEEE Access*, vol. 6, pp. 1706–1717, 2018.

[2] J. Boote. (2019). *Are You Making Software Security a Requirement?* Accessed: Aug. 17, 2019. [Online]. Available: https://www.synopsys.com/blogs/software-security/software-security-requirements/amp/

[3] T M Corporation. (2019). *Privacy Requirements Definition and Testing*. Accessed: Sep. 19, 2019. [Online]. Available: https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/engineering-informationintensive#targetText=Privacy%20testing%20is%20an%20important,ensure%20that%20systems%20protect%20PII.&targetText=Privacy%20requirements%20definition%20and%20testing%20are%20two%20such%20activities

[4] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE Access*, vol. 6, pp. 18209–18237, 2018.

[5] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Gener. Comput. Syst.*, vol. 78, pp. 680–698, Jan. 2018.

[6] Z. Guan, Y. Zhang, G. Si, Z. Zhou, J. Wu, S. Mumtaz, and J. Rodriguez, "ECOSECURITY: Tackling challenges related to data exchange and security: An edge-computing-enabled secure and efficient data exchange architecture for the energy Internet," *IEEE Consum. Electron. Mag.*, vol. 8, no. 2, pp. 61–65, Mar. 2019.

[7] R. Rapuzzi and M. Repetto, "Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model," *Future Gener. Comput. Syst.*, vol. 85, pp. 235–249, Aug. 2018.

[8] S. N. Shirazi, A. Gouglidis, A. Farshad, and D. Hutchison, "The extended cloud: Review and analysis of mobile edge computing and fog from a security and resilience perspective," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 11, pp. 2586–2595, Nov. 2017.

[9] J. Edwards. (2019). *Edge Computing Security Dos and Don'ts*. Accessed: Sep. 7, 2019. [Online]. Available: https://www.networkcomputing.com/network-security/edge-computing-security-dos-and-donts

[10] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[11] A. Yousefpour, C. Fung, T. Nguyen, K. Kadiyala, F. Jalali, A. Niakanlahiji, J. Kong, and J. P. Jue, "All one needs to know about fog computing and related edge computing paradigms: A complete survey," *J. Syst. Archit.*, vol. 98, pp. 289–330, Sep. 2019.

[12] B. Sudqi Khater, A. W. B. Abdul Wahab, M. Y. I. B. Idris, M. Abdulla Hussain, and A. Ahmed Ibrahim, "A lightweight perceptron-based intrusion detection system for fog computing," *Appl. Sci.*, vol. 9, no. 1, p. 178, 2019.

[13] K. P. Saharan and A. Kumar, "Fog in comparison to cloud: A survey," *Int. J. Comput. Appl.*, vol. 122, no. 3, pp. 10–12, 2015.

[14] I. Stojmenovic and S. Wen, "The fog computing paradigm: Scenarios and security issues," in *Proc. Federated Conf. Comput. Sci. Inf. Syst.*, Sep. 2014, pp. 1–8.

[15] Y. Wang, "The relationships among cloud computing, fog computing, and dew computing," Dew Comput. Res., Island Scholar Robertson Library, Tech. Rep., 2015.

[16] E. Borcoci, "Fog computing, mobile edge computing, cloudlets-which one," in *Proc. SoftNet Conf.*, 2016, pp. 1–122.

[17] Y. Ai, M. Peng, and K. Zhang, "Edge computing technologies for Internet of Things: A primer," *Digit. Commun. Netw.*, vol. 4, no. 2, pp. 77–86, Apr. 2018.

[18] M. Satyanarayanan, Z. Chen, K. Ha, W. Hu, W. Richter, and P. Pillai, "Cloudlets: At the leading edge of mobile-cloud convergence," in *Proc. 6th Int. Conf. Mobile Comput., Appl. Services*, 2014, pp. 1–9.

[19] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The case for VM-based cloudlets in mobile computing," *IEEE Pervas. Comput.*, vol. 8, no. 4, pp. 14–23, Oct. 2009.

[20] R. K. Barik, A. C. Dubey, A. Tripathi, T. Pratik, S. Sasane, R. K. Lenka, H. Dubey, K. Mankodiya, and V. Kumar, "Mist data: Leveraging mist computing for secure and scalable architecture for smart and connected health," *Procedia Comput. Sci.*, vol. 125, pp. 647–653, 2018.

[21] N. Angeline C. V. and R. Lavanya, "Fog computing and its role in the Internet of Things," in *Proc. 1st Ed. MCC Workshop Mobile Cloud Comput.* New York, NY, USA: ACM, 2012, pp. 63–71.

[22] C. Li, Y. Xue, J. Wang, W. Zhang, and T. Li, "Edge-oriented computing paradigms: A survey on architecture design and system management," *ACM Comput. Surv.*, vol. 51, no. 2, p. 39, Jun. 2018.

[23] A. Manzalini and N. Crespi, "An edge operating system enabling anything-as -a-service," *IEEE Commun. Mag.*, vol. 54, no. 3, pp. 62–67, Mar. 2016.

[24] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computing: A key technology towards 5G," *ETSI White Paper*, vol. 11, no. 11, pp. 1–16, 2015.

[25] A. Ahmed and E. Ahmed, "A survey on mobile edge computing," in *Proc. 10th Int. Conf. Intell. Syst. Control (ISCO)*, Coimbatore, India, Jan. 2016, pp. 1–8.

[26] A. Bahtovski and M. Gusev, "Cloudlet challenges," *Procedia Eng.*, vol. 69, pp. 704–711, Mar. 2014.

[27] J. S. Preden, K. Tammemae, A. Jantsch, M. Leier, A. Riid, and E. Calis, "The benefits of self-awareness and attention in fog and mist computing," *Computer*, vol. 48, no. 7, pp. 37–45, Jul. 2015.

[28] Y. Wang, "Definition and categorization of dew computing," *Open J. Cloud Comput.*, vol. 3, no. 1, pp. 1–7, 2016.

[29] Y. Pan and G. Luo, "Cloud computing, fog computing, and dew computing," *ZTE Commun.*, vol. 15, no. 4, pp. 1–2, 2017.

[30] T. H. Luan, L. Gao, Z. Li, Y. Xiang, G. Wei, and L. Sun, "Fog computing: Focusing on mobile users at the edge," 2015, *arXiv:1502.01815*. [Online]. Available: http://arxiv.org/abs/1502.01815

[31] K. Bilal, O. Khalid, A. Erbad, and S. U. Khan, "Potentials, trends, and prospects in edge technologies: Fog, cloudlet, mobile edge, and micro data centers," *Comput. Netw.*, vol. 130, pp. 94–120, Jan. 2018.

[32] G. I. Klas, *Fog Computing and Mobile Edge Cloud Gain Momentum Open Fog Consortium, ETSI MEC and Cloudlets*, document Open Fog Consortium-ETSI MEC-Cloudlets V1.docx, 2015.

[33] K. Skala, D. Davidović, E. Afgan, I. Sović, and Z. Šojat, "Scalable distributed computing hierarchy: Cloud, fog and dew computing," *Open J. Cloud Comput.*, vol. 2, no. 1, pp. 16–24, Mar. 2015.

[34] Y. Wang, "Cloud-dew architecture," *Int. J. Cloud Comput.*, vol. 4, no. 3, pp. 199–210, 2015.

[35] Y. Cherdantseva and J. Hilton, "A reference model of information assurance & security," in *Proc. Int. Conf. Availability, Rel. Secur.*, Sep. 2013, pp. 546–555.

[36] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 4, pp. 586–602, Oct. 2017.

[37] E. Park, "Understanding 'Authenticity' in records and information management: Analyzing practitioner constructs," *Amer. Archivist*, vol. 64, no. 2, pp. 270–291, Sep. 2001.

[38] R. K. L. Ko, B. S. Lee, and S. Pearson, "Towards achieving accountability, auditability and trust in cloud computing," in *Proc. Int. Conf. Adv. Comput. Commun.* Springer, 2011, pp. 432–444.

[39] A. JØsang, "A subjective metric of authentication," in *Proc. Eur. Symp. Res. Comput. Secur.* Springer, 1998, pp. 329–344.

[40] D. Xu, L. Xiao, L. Sun, and M. Lei, "Game theoretic study on blockchain based secure edge networks," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Oct. 2017, pp. 1–5.

[41] B. Han, S. Wong, C. Mannweiler, M. R. Crippa, and H. D. Schotten, "Context-awareness enhances 5G multi-access edge computing reliability," *IEEE Access*, vol. 7, pp. 21290–21299, 2019.

[42] Z. Ali, M. S. Hossain, G. Muhammad, I. Ullah, H. Abachi, and A. Alamri, "Edge-centric multimodal authentication system using encrypted biometric templates," *Future Gener. Comput. Syst.*, vol. 85, pp. 76–87, Aug. 2018.

[43] K. Saraswathi and R. Balasubramaniam, "BioCryptosystems for authentication and network security-a survey," *Global J. Comput. Sci. Technol.*, vol. 10, pp. 12–16, Apr. 2010.

[44] F. Hao, R. Anderson, and J. Daugman, "Combining cryptography with biometrics effectively," Dept. Comput. Lab., Univ. Cambridge, Cambridge, U.K., Tech. Rep. UCAM-CL-TR-640, 2005. [Online]. Available: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-640.pdf

[45] S. Chen, Y. Jiang, H. Wen, W. Liu, J. Chen, W. Lei, and A. Xu, "A novel terminal security access method based on edge computing for IoT," in *Proc. Int. Conf. Netw. Netw. Appl. (NaNA)*, Oct. 2018, pp. 394–398.

[46] X.-Y. Liu, S. Aeron, V. Aggarwal, X. Wang, and M.-Y. Wu, "Adaptive sampling of RF fingerprints for fine-grained indoor localization," *IEEE Trans. Mobile Comput.*, vol. 15, no. 10, pp. 2411–2423, Oct. 2016.

[47] S. U. Rehman, K. W. Sowerby, S. Alam, and I. Ardekani, "Radio frequency fingerprinting and its challenges," in *Proc. IEEE Conf. Commun. Netw. Secur.*, Oct. 2014, pp. 496–497.

[48] S. U. Rehman, K. Sowerby, and C. Coghill, "Analysis of receiver front end on the performance of RF fingerprinting," in *Proc. IEEE 23rd Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2012, pp. 2494–2499.

[49] S. U. Rehman, K. W. Sowerby, and C. Coghill, "Analysis of impersonation attacks on systems using RF fingerprinting and low-end receivers," *J. Comput. Syst. Sci.*, vol. 80, no. 3, pp. 591–601, May 2014.

[50] H. Cui, X. Yi, and S. Nepal, "Achieving scalable access control over encrypted data for edge computing networks," *IEEE Access*, vol. 6, pp. 30049–30059, 2018.

[51] H. Xiong, Y. Zhao, L. Peng, H. Zhang, and K.-H. Yeh, "Partially policy-hidden attribute-based broadcast encryption with secure delegation in edge computing," *Future Gener. Comput. Syst.*, vol. 97, pp. 453–461, Aug. 2019.

[52] W. Abdul, Z. Ali, S. Ghouzali, B. Alfawaz, G. Muhammad, and M. S. Hossain, "Biometric security through visual encryption for fog edge computing," *IEEE Access*, vol. 5, pp. 5531–5538, 2017.

[53] Y. Niu, J. Zhang, A. Wang, and C. Chen, "An efficient collision power attack on AES encryption in edge computing," *IEEE Access*, vol. 7, pp. 18734–18748, 2019.

[54] W. Xue, Y. Shen, C. Luo, W. Hu, and A. Seneviratne, "Acies: A privacy-preserving system for edge-based classification," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 914–919.

[55] H. Shen, G. Bai, Y. Hu, and T. Wang, "P2TA: Privacy-preserving task allocation for edge computing enhanced mobile crowdsensing," *J. Syst. Archit.*, vol. 97, pp. 130–141, Aug. 2019.

[56] N. Vance, D. Zhang, Y. Zhang, and D. Wang, "Privacy-aware edge computing in social sensing applications using ring signatures," in *Proc. IEEE 24th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2018, pp. 755–762.

[57] L. Ni, H. Lin, M. Zhang, and J. Zhang, "Hybrid filtrations recommendation system based on privacy preserving in edge computing," *Procedia Comput. Sci.*, vol. 129, pp. 407–409, Jan. 2018.

[58] X. He, J. Liu, R. Jin, and H. Dai, "Privacy-aware offloading in mobile-edge computing," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–6.

[59] A. Rahman, E. Hassanain, and M. S. Hossain, "Towards a secure mobile edge computing framework for Hajj," *IEEE Access*, vol. 5, pp. 11768–11781, 2017.

[60] H. Jiang, H. Wang, Z. Zheng, and Q. Xu, "Privacy preserved wireless sensor location protocols based on mobile edge computing," *Comput. Secur.*, vol. 84, pp. 393–401, Jul. 2019.

[61] P. Zhang, M. Durresi, and A. Durresi, "Mobile privacy protection enhanced with multi-access edge computing," in *Proc. IEEE 32nd Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, May 2018, pp. 724–731.

[62] P. Zhang, M. Durresi, and A. Durresi, "Network location privacy protection with multi-access edge computing," in *Proc. Int. Conf. Adv. Inf. Netw. Appl.* Springer, 2019, pp. 1342–1352.

[63] T. He, E. N. Ciftcioglu, S. Wang, and K. S. Chan, "Location privacy in mobile edge clouds," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2017, pp. 2264–2269.

[64] T. He, E. N. Ciftcioglu, S. Wang, and K. S. Chan, "Location privacy in mobile edge clouds: A chaff-based approach," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 11, pp. 2625–2636, Nov. 2017.

[65] T. Freitas, J. Rodrigues, D. Bogas, M. Coimbra, and R. Martins, "Panoptic, privacy over edge-clouds," in *Proc. IEEE 6th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2018, pp. 325–332.

[66] L. Zhou, L. Yu, S. Du, H. Zhu, and C. Chen, "Achieving differentially private location privacy in edge-assistant connected vehicles," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4472–4481, Jun. 2019.

[67] R. Xu, B. Palanisamy, and J. Joshi, "QueryGuard: Privacy-preserving latency-aware query optimization for edge computing," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 1097–1106.

[68] K. Gai, M. Qiu, Z. Xiong, and M. Liu, "Privacy-preserving multi-channel communication in edge-of-things," *Future Gener. Comput. Syst.*, vol. 85, pp. 190–200, Aug. 2018.

[69] X. Xu, Y. Xue, L. Qi, Y. Yuan, X. Zhang, T. Umer, and S. Wan, "An edge computing-enabled computation offloading method with privacy preservation for Internet of connected vehicles," *Future Gener. Comput. Syst.*, vol. 96, pp. 89–100, Jul. 2019.

[70] Q. Xu, Z. Su, Y. Wang, and M. Dai, "A trustworthy content caching and bandwidth allocation scheme with edge computing for smart campus," *IEEE Access*, vol. 6, pp. 63868–63879, 2018.

[71] Q. Xu, Z. Su, Q. Zheng, M. Luo, and B. Dong, "Secure content delivery with edge nodes to save caching resources for mobile users in green cities," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2550–2559, Jun. 2018.

[72] M. A. Rahman, M. S. Hossain, G. Loukas, E. Hassanain, S. S. Rahman, M. F. Alhamid, and M. Guizani, "Blockchain-based mobile edge computing framework for secure therapy applications," *IEEE Access*, vol. 6, pp. 72469–72478, 2018.

[73] D. Puthal, R. Ranjan, A. Nanda, P. Nanda, P. P. Jayaraman, and A. Y. Zomaya, "Secure authentication and load balancing of distributed edge datacenters," *J. Parallel Distrib. Comput.*, vol. 124, pp. 60–69, Feb. 2019.

[74] X. Ma and X. Li, "Trust evaluation model in edge computing based on integrated trust," in *Proc. Int. Conf. Algorithms, Comput. Artif. Intell. (ACAI)*. New York, NY, USA: ACM, 2018, p. 26.

[75] F. N. Nwebonyi, R. Martins, and M. E. Correia, "Reputation-based security system for edge computing," in *Proc. 13th Int. Conf. Availability, Rel. Secur. (ARES)*. New York, NY, USA: ACM, 2018, p. 39.

[76] J. Yuan and X. Li, "A reliable and lightweight trust computing mechanism for IoT edge devices based on multi-source feedback information fusion," *IEEE Access*, vol. 6, pp. 23626–23638, 2018.

[77] Y. Ruan, A. Durresi, and S. Uslu, "Trust assessment for Internet of Things in multi-access edge computing," in *Proc. IEEE 32nd Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, May 2018, pp. 1155–1161.

[78] K. Mahmood, X. Li, S. A. Chaudhry, H. Naqvi, S. Kumari, A. K. Sangaiah, and J. J. P. C. Rodrigues, "Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure," *Future Gener. Comput. Syst.*, vol. 88, pp. 491–500, Nov. 2018.

[79] H. Li and L. Wang, "Online orchestration of cooperative defense against DDoS attacks for 5G MEC," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2018, pp. 1–6.

[80] B. Li, T. Chen, X. Wang, and G. B. Giannakis, "Secure edge computing in IoT via online learning," in *Proc. 52nd Asilomar Conf. Signals, Syst., Comput.*, Oct. 2018, pp. 2149–2153.

[81] H. Sedjelmaci, I. Ben Jemaa, M. Hadji, and A. Kaiser, "Security framework for vehicular edge computing network based on behavioral game," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6.

[82] Q. Li, S. Meng, S. Zhang, J. Hou, and L. Qi, "Complex attack linkage decision-making in edge computing networks," *IEEE Access*, vol. 7, pp. 12058–12072, 2019.

[83] S. Xia, N. Li, T. Xiaofeng, and C. Fang, "Multiple attributes based spoofing detection using an improved clustering algorithm in mobile edge network," in *Proc. 1st IEEE Int. Conf. Hot Inf.-Centric Netw. (HotICN)*, Aug. 2018, pp. 242–243.

[84] R. Kozik, M. Choraś, M. Ficco, and F. Palmieri, "A scalable distributed machine learning approach for attack detection in edge computing environments," *J. Parallel Distrib. Comput.*, vol. 119, pp. 18–26, Sep. 2018.

[85] A. Mtibaa, K. Harras, and H. Alnuweiri, "Friend or foe? Detecting and isolating malicious nodes in mobile edge computing platforms," in *Proc. IEEE 7th Int. Conf. Cloud Comput. Technol. Sci. (CloudCom)*, Nov. 2015, pp. 42–49.

[86] J. Abawajy, S. Huda, S. Sharmeen, M. M. Hassan, and A. Almogren, "Identifying cyber threats to mobile-IoT applications in edge computing paradigm," *Future Gener. Comput. Syst.*, vol. 89, pp. 525–538, Dec. 2018.

[87] Q. Wang, Z. Lu, M. Gao, and G. Qu, "Edge computing based GPS spoofing detection methods," in *Proc. IEEE 23rd Int. Conf. Digit. Signal Process. (DSP)*, Nov. 2018, pp. 1–5.

[88] Z. Tang, M. Xue, G. Meng, C. Ying, Y. Liu, J. He, H. Zhu, and Y. Liu, "Securing Android applications via edge assistant third-party library detection," *Comput. Secur.*, vol. 80, pp. 257–272, Jan. 2019.

[89] X. Wang, H. Xue, X. Liu, and Q. Pei, "A privacy-preserving edge computation-based face verification system for user authentication," *IEEE Access*, vol. 7, pp. 14186–14197, 2019.

[90] Z. Wang, "A privacy-preserving and accountable authentication protocol for IoT end-devices with weaker identity," *Future Gener. Comput. Syst.*, vol. 82, pp. 342–348, May 2018.

[91] P. Zhou, K. Wang, J. Xu, and D. Wu, "Differentially-private and trustworthy online social multimedia big data retrieval in edge computing," *IEEE Trans. Multimedia*, vol. 21, no. 3, pp. 539–554, Mar. 2019.

[92] T. Gao, Y. Li, N. Guo, and I. You, "An anonymous access authentication scheme for vehicular ad hoc networks under edge computing," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 2, Feb. 2018, Art. no. 155014771875658.

[93] V. Sharma, I. You, D. N. K. Jayakody, and M. Atiquzzaman, "Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social Internet of Things," *Future Gener. Comput. Syst.*, vol. 92, pp. 758–776, Mar. 2019.

[94] X. Li, S. Liu, F. Wu, S. Kumari, and J. J. P. C. Rodrigues, "Privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4755–4763, Jun. 2019.

[95] J. Zhang, Y. Zhao, J. Wu, and B. Chen, "LPDA-EC: A lightweight privacy-preserving data aggregation scheme for edge computing," in *Proc. IEEE 15th Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, Oct. 2018, pp. 98–106.

[96] A. Celesti, M. Fazio, A. Galletta, L. Carnevale, J. Wan, and M. Villari, "An approach for the secure management of hybrid cloud–edge environments," *Future Gener. Comput. Syst.*, vol. 90, pp. 1–19, Jan. 2019.

[97] S. Almajali, H. B. Salameh, M. Ayyash, and H. Elgala, "A framework for efficient and secured mobility of IoT devices in mobile edge computing," in *Proc. 3rd Int. Conf. Fog Mobile Edge Comput. (FMEC)*, Apr. 2018, pp. 58–62.

[98] X. Huang, R. Yu, M. Pan, and L. Shu, "Secure roadside unit hotspot against eavesdropping based traffic analysis in edge computing based Internet of vehicles," *IEEE Access*, vol. 6, pp. 62371–62383, 2018.

[99] G. Li, H. Zhou, B. Feng, G. Li, T. Li, Q. Xu, and W. Quan, "Fuzzy theory based security service chaining for sustainable mobile-edge computing," *Mobile Inf. Syst.*, vol. 2017, pp. 1–13, Feb. 2017.

[100] X. Zhang, R. Li, and B. Cui, "A security architecture of VANET based on blockchain and mobile edge computing," in *Proc. 1st IEEE Int. Conf. Hot Inf.-Centric Netw. (HotICN)*, Aug. 2018, pp. 258–259.

[101] A. H. Celdran, F. J. Garcia Clemente, J. Weimer, and I. Lee, "ICE++: Improving security, QoS, and high availability of medical cyber-physical systems through mobile edge computing," in *Proc. IEEE 20th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Sep. 2018, pp. 1–8.

[102] A. Singh, N. Auluck, O. Rana, A. Jones, and S. Nepal, "RT-SANE: Real time security aware scheduling on the network edge," in *Proc. the10th Int. Conf. Utility Cloud Comput. (UCC)*. New York, NY, USA: ACM, 2017, pp. 131–140.

[103] B. Huang, Z. Li, P. Tang, S. Wang, J. Zhao, H. Hu, W. Li, and V. Chang, "Security modeling and efficient computation offloading for service workflow in mobile edge computing," *Future Gener. Comput. Syst.*, vol. 97, pp. 755–774, Aug. 2019.

[104] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access*, vol. 5, pp. 25408–25420, 2017.

[105] T. Nandy, M. Y. I. B. Idris, R. M. Noor, L. M. Kiah, L. S. Lun, N. B. A. Juma'at, I. Ahmedy, N. A. Ghani, and S. Bhattacharyya, "Review on security of Internet of Things authentication mechanism," *IEEE Access*, vol. 7, pp. 151054–151089, 2019.

[106] A. Ben Amor, M. Abid, and A. Meddeb, "A privacy-preserving authentication scheme in an edge-fog environment," in *Proc. IEEE/ACS 14th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Oct. 2017, pp. 1225–1231.

[107] C. Aggarwal and K. Srivastava, "Securing IOT devices using SDN and edge computing," in *Proc. 2nd Int. Conf. Next Gener. Comput. Technol. (NGCT)*, Oct. 2016, pp. 877–882.

[108] J. Yoon, "Trustworthiness of dynamic moving sensors for secure mobile edge computing," *Computers*, vol. 7, no. 4, p. 63, 2018.

[109] J. Yuan and X. Li, "A multi-source feedback based trust calculation mechanism for edge computing," in *Proc. IEEE INFOCOM-IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2018, pp. 819–824.

[110] W. J. Buchanan, S. Li, and R. Asif, "Lightweight cryptography methods," *J. Cyber Secur. Technol.*, vol. 1, nos. 3–4, pp. 187–201, Sep. 2017.

[111] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Elliptic curve lightweight cryptography: A survey," *IEEE Access*, vol. 6, pp. 72514–72550, 2018.

MUKTAR YAHUZA was born in Nguru, Yobe, Nigeria, in 1984. He received the B.Eng. degree in computer engineering from Bayero University Kano, Nigeria, in 2010, and the M.Sc. degree in computer information and engineering from International Islamic University Malaysia (IIUM), in 2015. He is currently pursuing the Ph.D. degree in computer science with the University of Malaya, Malaysia.

His areas of research include smart environment authentication, information security, and image processing.

MOHD YAMANI IDNA BIN IDRIS (Member, IEEE) received the B.E. M.Sc., and Ph.D. degrees in electrical engineering from the University of Malaya, Kuala Lumpur, Malaysia.

He is currently an Associate Professor with the Department of Computer Systems, Faculty of Computer Science and Information Technology, University of Malaya. He is the author of a book, more than 110 articles in reputable journals, and more than 20 inventions. His research interests include information security, embedded systems (system on chip and FPGA), image processing and computer vision, digital forensics, surveillance systems, digital signal processing (speech processing and bio-signals), and wireless sensor networks.

AINUDDIN WAHID BIN ABDUL WAHAB (Member, IEEE) received the B.Sc. and M.Sc. degrees in computer science from the University of Malaya, Kuala Lumpur, Malaysia, and the Ph.D. degree in multimedia network from Surrey University, U.K.

He is currently working as an Associate Professor and the Deputy Dean (Undergraduate) with the Department of Computer Systems, Faculty of Computer Science and Information Technology, University of Malaya, Malaysia. He published more than 90 articles in reputable journals. His areas of expertise include information security, network security, information hiding, digital forensics, steganography, and sensor networks. He is an Associate Editor of *Journal of Information Security and Applications* (JISA) (Elsevier).

ANTHONY T. S. HO (Senior Member, IEEE) was born in Hong Kong, in 1977. He received the B.Sc. degree (Hons.) in physical electronics from Northumbria University, in 1979, the M.Sc. degree in applied optics from Imperial College London, in 1980, and the Ph.D. degree in digital image processing from King's College London, in 1983.

He has published more than 160 articles in international journals and conference proceedings and eight international patents granted related to watermarking and steganography. He is a co-editor of a book on "Handbook of Digital Forensics of Multimedia Data and Devices" (Wiley-IEEE press, September 2015). His research interests include multimedia security, image forensics, digital watermarking, and steganalysis.

Prof. Ho was a recipient of the prestigious Institution of Engineering and Technology (IET) under the Security category for his research and commercialization work on digital watermarking, in 2006. Under his leadership, Surrey Computer Science has been ranked four consecutive years as one of the top 150 Computer Science Departments in the World, won the bid to host the flagship IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2019 in Brighton, UK. He received the best paper award for a coauthored conference paper on camera model identification from IEVC 2012. He is the founding Editor-in-Chief of international *Journal of Information Security and Applications* (JISA).

SULEMAN KHAN (Member, IEEE) received the Ph.D. degree (Hons.) from the Faculty of Computer Science and Information Technology, University of Malaya, Malaysia, in 2017. He was a Faculty Member with the School of Information Technology, Monash University Malaysia, from June 2017 to March 2019. He is currently a Faculty Member with the Department of Computer and Information Sciences, Northumbria University, Newcastle, U.K. He has published more than 60 high-impact research articles in reputed international journals and conferences. His research areas include, but are not limited to, network forensics, software-defined networks, the Internet of Things, cloud computing, and vehicular communications.

SITI NURMAYA BINTI MUSA received the bachelor's degree in industrial engineering from the University of Wisconsin-Milwaukee, USA, the master's degree in manufacturing engineering and management from the University of Nottingham, U.K, and the Ph.D. degree in production economics from Linköping University, Sweden.

She is currently a Senior Lecturer at the Department of Mechanical Engineering, University of Malaya, Malaysia. Her areas of expertise are supply chain risk management, manufacturing management, production and logistics, production economics, operations research, and management science.

AZNI ZARINA BINTI TAHA received the B.Sc. degree from the University of Missouri, Columbia, USA, the M.B.A. degree from the University of Malaya, Malaysia, and the Ph.D. degree from Aston University, U.K.

She teaches a range of management subjects which include strategic management, services, and tourism. Besides teaching, she is actively involved in projects and research consultancy. Some of the projects include the development of strategic customer service roadmap for Kumpulan Wang Amanah Pekerja (KWAP), and profiling of mosques as tourism attractions for Islamic Tourism Centre of Ministry of Tourism and Culture.