Received: 3 April 2023 | Revised: 14 August 2023 | Accepted: 29 August 2023

DOI: 10.1002/ett.4861

Security analysis of fog computing environment for ensuring the security and privacy of information

Kamal Kumar Gola[1] | **Shikha Arya**[2] | **Gulista Khan**[3] | **Chetna Devkar**[4] | **Nishant Chaurasia**[5]

[1]COER University, Roorkee, Uttarakhand, India

[2]Indian Institute of Technology, Roorkee, Uttarakhand, India

[3]Teerthanker Mahaveer University, Moradabad, India

[4]Rabindranath Tagore University, Bhopal, India

[5]Dr. B R Ambedkar National Institute of Technology, Jalandhar, Punjab, India

Correspondence
Kamal Kumar Gola, COER University, Roorkee, 247667, Uttarakhand, India.
Email: kkgolaa1503@gmail.com

Abstract

In fog computing, the management, measurement, configuration, control, communication, and storage tasks are carried out collaboratively by one or more near-user or end users. Fog computing is widely utilized in major application domains like centralized fog utilized in a shopping complex (UXFog), agriculture domain (FoAgro), health-care domain (MediFog), vehicle parking system, and energy Lattices. The execution of fog computing at the system's edge provides the elevated quality of service (QoS), promotes area mindfulness, and minimal dormancy for the continuous and online streaming application areas. Fog networking is extremely concerned about wireless system security due to the prevalence of wireless communication in fog computing. Sniffer attacks, Jamming assaults, and several other intrusions are considered examples of security issues. While considering network storage issues, factors like interaction management, dynamic workload, and low dormancy are the most challenging aspects of designing the network model. Thus, privacy and security issues are crucial while designing the network model, accomplished through intrusion detection, access control and authentication methods. Therefore, the security analysis of fog computing based on authentication, access control and intrusion detection mechanisms are analyzed in this research to design a novel technique with enhanced security and privacy features for sharing and accessing information.

1 | INTRODUCTION

Systems that can administer the network, store the data and process during the past few years employed using cloud computing and have recently become popular. Cloud computing utilizes centralized data centers to perform various control tasks.[1] Due to growing demand and low cost, cloud computing has been utilized across various industries and become more popular with consumers and businesses. Thus, the cloud became one of the essential criteria in business organizations and scaled up successfully worldwide.[2] At the precise location, the cloud supplies the right resources; hence, the IT teams' work decreases enormously, boosting an organization's productivity. The reliable, secure and precise performance of cloud computing benefits organization outcomes. Software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) are the services provided by cloud computing. Over the past several years, a huge increase in cloud users has resulted in a significant demand for IoT.[3] With billions of IoT devices connected through the cloud, centralized processing frequently makes the network struggle.[4] Issues like poor service quality, excessive latency, and network congestion make the inability to process real-time services, leading to the development of fog computing.[5]

Information is stored and prepared among the network equipment as well as source point in fog computing utilizes a distributed system paradigm.[6] The information transmission overheads of fog are minimized through the elevated computing capability by preventing the need to process and store large amounts of redundant information. The idea of fog computing is typically driven by an enduring rise in Internet of Things (IoT) devices; an ever-growing amount of data is produced by a cluster of devices constantly growing. IoT devices offer a wide range of benefits, like developing new benefits that frequently spark information and availability.[7] However, edge devices also need quick decision processes to sustain an abnormal requirement. Computing resources are needed to process the acquired information by edge devices. At the same time, using typical customer-server engineering, wherein the server manages the information identified by the user, which displays unwavering and adaptability quality difficulties.[8] Numerous devices might become inoperable if a server gets overloaded in a typical customer server configuration. To address this problem, the Fog worldview intends to provide a flexible, decentralized solution.[9]

Unquestionably, fog computing is a flexible, resource-rich, and variable environment-adapted network for efficient data sharing. However, its widespread distribution and open structural design expose it to various threats, jeopardizing the operation's security and safety.[10] In the IoT, fog nodes commonly comprise machines where information or data sharing takes place for the entire model based on trust. As a result, all processes and apps operating on fog benefit from efficient data sharing based on trust.[11] Various attacker scenarios can cripple the fog's application architecture without a technical base of confidence that would allow those attackers to seize control. Hence, more risky problems with safety and trust have emerged due to the fog's emergence.[12] A common attack in fog computing termed man-in-the-middle is considered as one of the potential attack that captures the confidential information by intercepting the communication. As an example of the security issues of fog computing based on the man-in-the-middle attack. Gateways acting as Fog devices in this attack could be compromised or taken out and replaced with fraudulent ones.[13] Customers of Star Bar or KFC, for instance, connecting to attacker access points that display false SSIDs as public real ones. Once the attackers take over the gateways, the victims' private communications will be intercepted.[14] The widespread universal dispersion, mobility, and diversity of fog make security issues related to information a threat. The security issues led to the study of privacy and security concerns related to issues in fog computing.[15] Besides, the confidentiality of information sharing must be enhanced through a deep analysis of the prior security analysis techniques regarding privacy and security. Here, different features of fog computing, such as its architecture, the layers involved, security and privacy issues, and other difficulties, must be analyzed to enhance the security model. Fog computing can be used effectively, but security and privacy issues must be addressed.[16]

The research organization is as follows: Section 2 details the architecture of a fog computing environment, and its layered model is presented in Section 3. The security issues and techniques utilized to solve the security and privacy issues, along with their categorization, are detailed in Section 4. The challenges faced by the prior methods are presented in section 5, and Section 6 details the future scope. Finally, Section 7 concludes the research.

2 | SYSTEMATIC ARTICLE SELECTION FOR SECURITY ANALYSIS OF FOG COMPUTING ENVIRONMENT

The fog computing is considered as the recent technique that extends the performance of the cloud computing. Improved data streaming, wireless connectivity, geographical accessibility, reduced latency, and location sensitivity of fog computing are considered as the added benefits. Still, the security and privacy issues limit the fog computing paradigm and hence the security analysis of the fog computing environment is proposed in this research. For the analysis of security and privacy constraints of the fog computing, the article inclusion and exclusion criteria are depicted in Figure 1.

Inclusion criteria: The research articles for the analysis of security in the fog computing environment are acquired through various databases using the search terms named keywords such as security analysis, privacy analysis, fog computing, deep learning, authentication and access control. Thus, using the keyword based search, a total of 1000 articles are gathered for the systematic review of the proposed security analysis of fog computing environment.

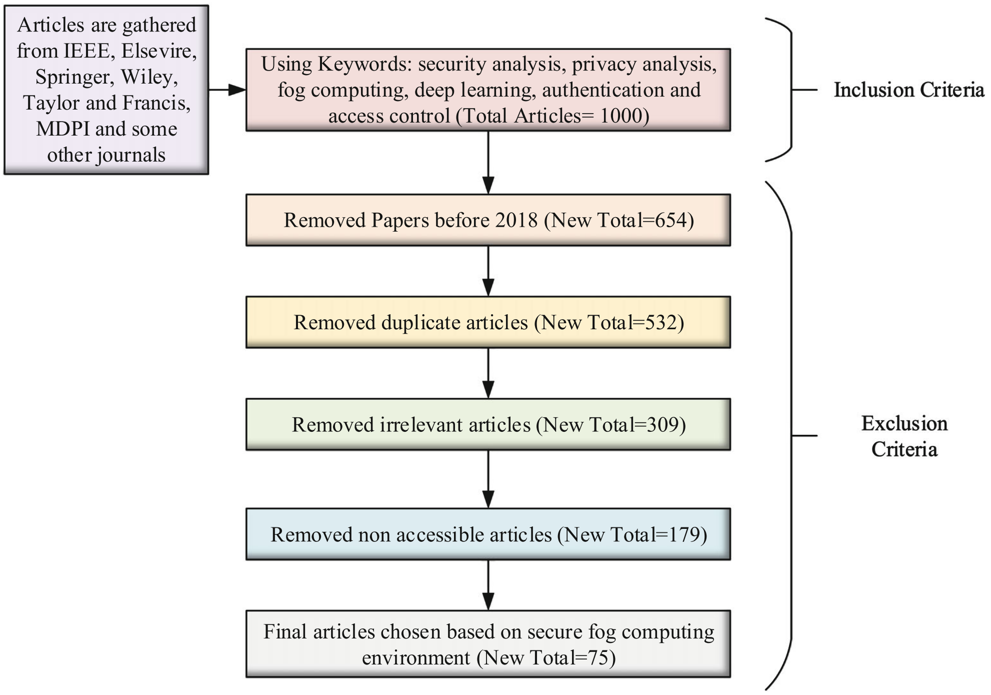
Articles are gathered from IEEE, Elsevire, Springer, Wiley, Taylor and Francis, MDPI and some other journals
Using Keywords: security analysis, privacy analysis, fog computing, deep learning, authentication and access control (Total Articles= 1000)
Inclusion Criteria
Removed Papers before 2018 (New Total=654)
Removed duplicate articles (New Total=532)
Removed irrelevant articles (New Total=309)
Removed non accessible articles (New Total=179)
Final articles chosen based on secure fog computing environment (New Total=75)
Exclusion Criteria

FIGURE 1 Systematic review article selection criteria.

Exclusion criteria: The gathered 1000 articles, are analyzed initially based on the year of publication and hence a total of 654 are selected by removing the articles before 2018. Then, the articles that are duplicated are removed and a total of 532 articles are obtained in this stage. Followed by, 223 research articles are removed that are irrelevant for the proposed security analysis; thus, a total of 309 articles are obtained in this stage. Then, the not accessible articles are removed and hence 179 articles are acquired in this stage. Finally, by removing the articles other than the fog computing environment are removed and utilized 75 articles for reviewing the security analysis of the proposed method.

3 | FOG COMPUTING ARCHITECTURE

The fog computing architecture considered for analyzing security issues is categorized into hierarchical fog computing architecture and multilayered architecture.

3.1 | Hierarchical architecture of fog computing

The edge, fog, and cloud layers constitute modern fog computing architecture, depicted in Figure 2.[17] Here, the topmost layer is a cloud, and the edge layer is at the bottom of the architecture. The fog layer is located between an edge and the cloud. The communication among the devices is employed among the fog–edge, fog–cloud, and fog–fog layers, wherein the communication is bidirectional.

3.1.1 | The cloud

Big data analysis, data warehousing, and broadcasting are employed using cloud storage devices and servers that offer high-performance information sharing. The information processing based on non-urgent tasks, complex data and high storage is employed using the management and remote control cloud server. The communication utilized by the cloud is devised through a wired or wireless high-speed network, wherein global coverage is the goal behind the cloud.

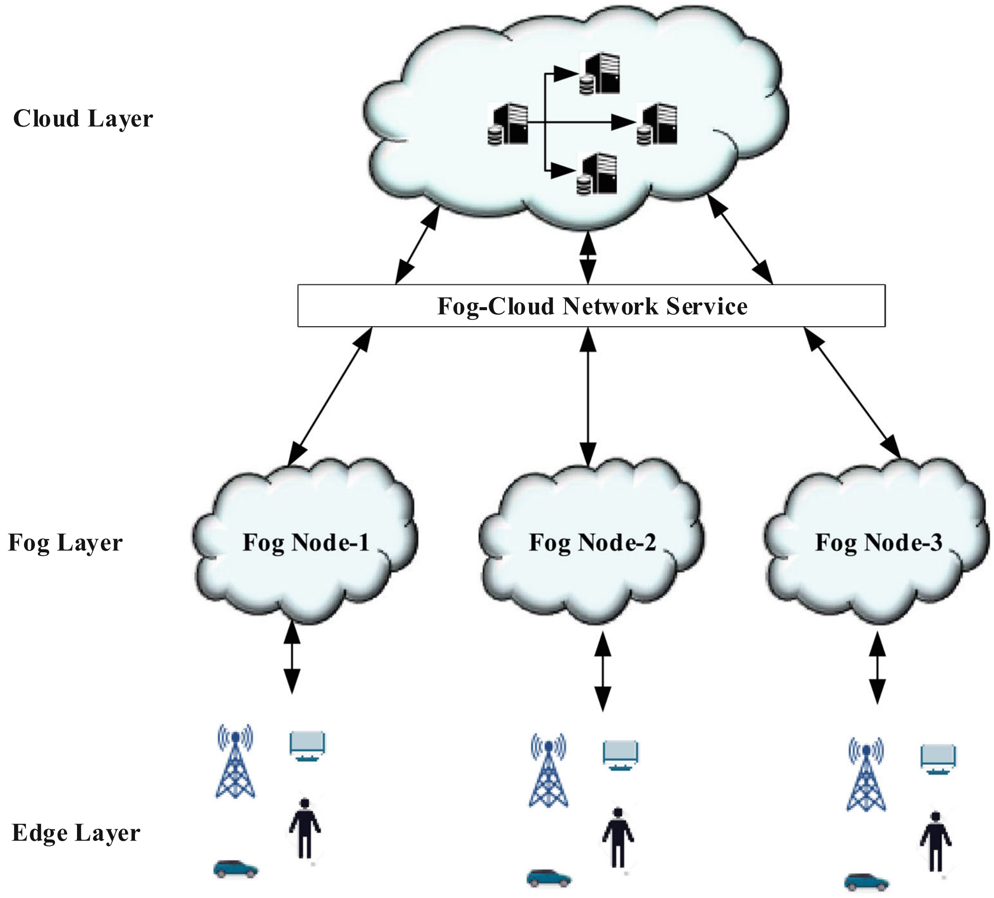

FIGURE 2 Hierarchical architecture of fog computing.

The cloud provides functionalities like intelligent data analysis and long-term consumer needs with efficient storage as an information repository.[18]

3.1.2 | The fog

A system with connected fog devices makes up the fog computing system. Geographical knowledge is offered along with urgent computation, low latency, and geo-distributed for efficient information sharing. For temporary retention of information, every node functions as a service hub. Additionally, fog devices perform monitoring, computing, data storage, information uploading, networking, extracting information, and networking transformation processing. Fog nodes process a sizable volume of data from edge devices due to an enhanced computer storage or memory capacity compared to the end devices.[19]

3.1.3 | The edge

Several physical devices like cell phones, machines and vehicles are connected in the edge layer, offering services like communication, sensing and identification. The devices in the edge layer are linked with the fog node, in which several sensors are connected to gather the information. The information gathered by the sensors shared directly with the cloud is time-consuming and expensive; hence, the urgently required data is processed by the fog without sharing it immediately.[20]

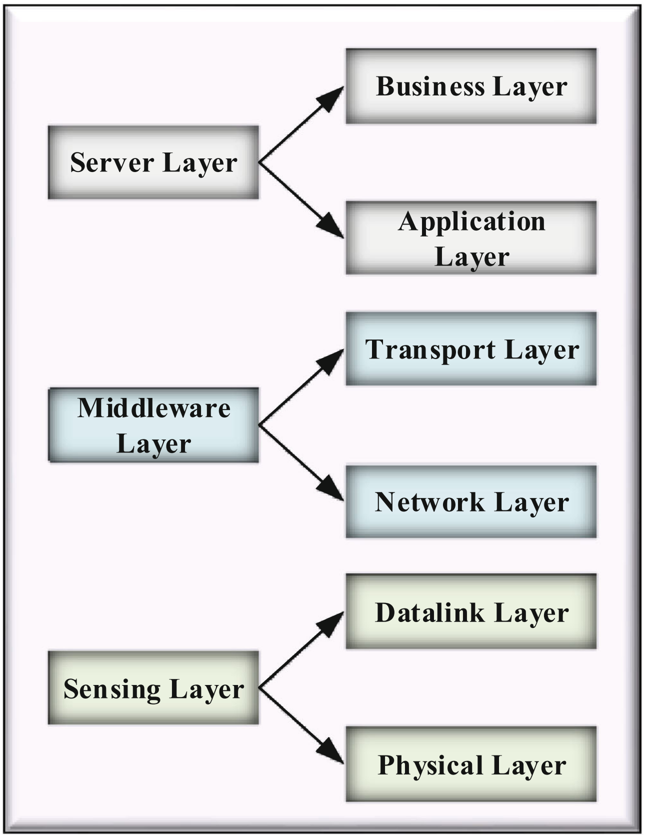

FIGURE 3 Layered model of fog.

3.1.4 | Fog vs. Edge computing

The information exchange between the end users and the cloud data centers is employed through the fog layer, wherein the networking, storage and computation services are offered. The computation power and intelligent data processing are similar for fog and edge devices. Data processing locations differ for both the fog and edge computing environments. Fog nodes utilize the local area network (LAN) for data processing; in contrast, the edge computing nodes devise the data processing in edge devices themselves.[21]

3.2 | Multilayered fog architecture

The layered architecture of fog computing comprises a sensing layer, middleware layer and fog server, depicted in Figure 3.[22]

3.2.1 | Sensing layer

The bottommost layers with the sensing devices constitute the sensing layer, designed by combining the datalink and communication layer. Some of the technologies like near-field communications (NFC), wireless sensor networks (WSN), and radio frequency identification (RFID) tags are utilized as the sensing technologies for developing the infrastructure.[23]

3.2.2 | Middleware

The layer between the fog server and the bottom application layer constitute the middleware layer, which comprises the transport and network layer. The information is processed by the Zigbee, Bluetooth, and Wi-Fi transmission medium through wired or wireless communication.[24] The functionalities of the middleware layer are:

1. With the help of network connectivity, the information gathered by the sensing layer is processed.
2. The information transfers to the fog server layer, acquired from the sensing layer.
3. Secure information sharing.

3.2.3 | Fog server

The business and application layers are the two categories of a fog server layer. The management of application processing is a major function and acts as the user's front-end layer. Banking, health, and transportation are some applications processed by the fog server deploying IoT applications. Here, the security issues are managed by the business fog server layer.[25]

4 | SECURITY AND PRIVACY ISSUES

The characteristics of fog computing, like limited resources, mobility, heterogeneity, and distribution behavior generate privacy and security-related issues. The low power capability of a network model makes attack detection and its mitigation as a challenging task. Besides, the location-aware network design elevates the possibility of attack due to weak surveillance and protection schemes. Thus, various kinds of attacks affect the privacy and security of a model.[26–32] The various types of attacks in the fog computing network are:

Sybil attack: In this attacking strategy, the intruder attacks a node in the network and generates several illegal identities to capture confidential information.

Node replication attack: The intruder devised the replica of an attacked node to capture the sensitive information performed in the node replication attack.

Wormhole attack: The information shared by the intruder is transmitted from one location to another through the network and retransmits the information to the particular device to capture the information.

Sinkhole attack: The intruder acts like the neighboring node, misguides the information routing, and captures the information shared through the intruder node.

Replay attack: For the authorized user in the network, the intruder sends the replay message for the earlier shared message to capture the secure information.

Man-in-the-middle attack: The information altering by interrupting the communication between two users is employed by the man-in-the-middle attack. In this, the attacker can perform the message injection and deletion.

Impersonation attack: In this attacking strategy, the network intruder shares the forged message to the other network devices on behalf of the authenticated source entity to capture the sensitive information.

Privileged-insider attack: The sensitive information threat by the user within the network is considered a privileged-insider attack. Here, the intruder may be the employee of an organization.

Online/offline guessing attacks: Credential capturing is the goal behind an online/offline guessing attack. The captured authenticated outcome employs the possible guesses to log into the device.

Ephemeral secret leakage (ESL) attack: The public key of a user is captured by the intruder by compromising the ephemeral secrets. Thus, confidential information is attacked by the eavesdropper.

Device capture attack: In this attacking strategy, the intruder attacks a device in the network directly. Then all devices in the network are attacked using the credentials of a particular device, so security becomes a challenging task.

4.1 | Conventional attack handling methods

This section details prior methods devised by the researchers to handle various attacks detailed in Section 4. The anomaly detection and mitigation approach devised by[33] handles various attacks like Man-in-the-middle, false data injection, denial of service (DoS), Sybil, brute force and replay attacks through the authentication approach. In this, the trusted user categorization was accomplished through fuzzy logic. The devised method outperformed based on memory and computation cost; the slow learning and inability to identify the new attack types related to the attack family limits the model's performance. An attack detection and mitigation method devised by[34] can handle probe attacks, Sybil attacks, black hole attacks, and other attacks using the rule-based clustering technique. An immediate restriction application employed the isolation of an identified attacker. The prediction accuracy of a method was higher; still, the computation overhead limits the performance. An end-to-end secure system designed by[35] to handle various attacks like man-in-the-middle, spoofing, and replay attacks through the collaborative learning and cryptographic system. The enhanced security with minimal network overhead depicts the superiority of a model. Still, the inability to detect new attacks due to sparsity limits the performance of a model.

4.2 | Fog-assisted application domains

The conventional methods utilized in fog computing with security features are detailed in this section.

Smart agriculture: A deep learning-based method devised by[36] to detect DDoS attacks in the smart agriculture application. The attacker makes the service unavailability through the DDoS attack, identified by the hybrid classifier designed by combining RNN, CNN and DNN. The introduced method acquired a higher accuracy for multi and binary classification. The computation overhead and vanishing gradient issues limit the model's performance.

Smart vehicular communication: An authentication-based secure communication among the smart vehicles in the fog computing scenario was devised by.[37] The user behavior profiling algorithm minimized the network insider attack in the introduced model. The model's superiority was evaluated based on the false positive measure; still, the failure to consider the essential attributes limits performance.

Smart healthcare: A deep learning hybrid model that combines CNN and BiLSTM for secure information sharing in fog computing situations.[38] The health-care information acquired from various sources in heterogeneous data was represented contextually using the medical entity recognition criteria. Followed by the model's privacy was ensured through the medical entity sanitization approach. The performance was assessed by preserving utility that depicts the introduced method's performance. However, the analysis based on privacy was minimal compared to the conventional baseline methods.

The present-day security analysis is devised mostly based on the deep learning mechanism as mentioned above, but the traditional application domains utilize the instruction-based intrusion detection mechanism,[39] TCPDump-based mechanism,[40] and applied cognitive task analysis.[41] The traditional intrusion detection methods did not utilize any machine learning mechanisms; instead, some instructions and conditions were utilized to detect the intrusion in the network.

5 | TECHNIQUES TO OVERCOME THE SECURITY ISSUES OF FOG

As more IoT gadgets are added, the amount of data produced by edge or IoT devices increases, which leads to communication overhead. Processing all information on connected systems is challenging due to the limited resources available for IoT devices. The information shared among the network devices is employed through the closest fog node corresponding to the IoT network. The gathered information by the IoT devices is then segmented through this network into various portions and delivered to various fog nodes for additional processing. Adversaries might change or modify the data during the separation and transmission phase. So, it's important to guarantee the information's security while sharing the information. The decryption and encryption procedure of information securing is challenging due to resource limitations. The three-tier architecture is utilized for fog computing applications like intrusion detection, traffic analysis and monitoring.[42] Thus, several techniques were devised by researchers to enhance the security of fog computing.

5.1 | Categorization of security analysis mechanisms

The security analysis of a proposed fog computing environment is categorized into three types: authentication, access control and intrusion detection depicted in Figure 4.

Authentication: Identification of the legitimate user is accomplished through the authenticated network layer. With the help of credentials like passwords, the authentication of information access is ensured.[43]

Access control: Unauthorized access to the system is controlled through the access control mechanism that ensures the privacy and security of the model.

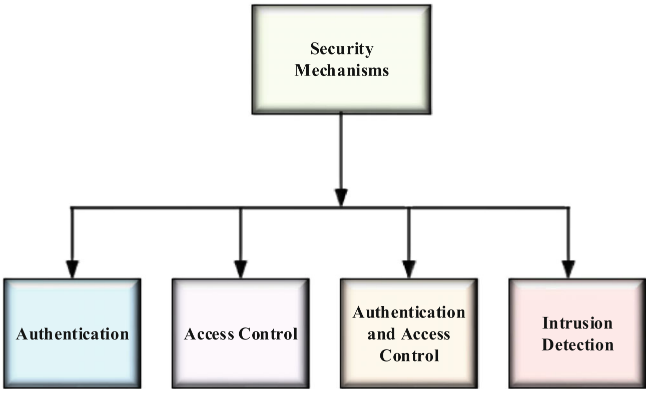

FIGURE 4 Categorization of security mechanisms.

The difference between authentication and access control is: Verification of an authorized user through the credentials employed through the authentication, and permission to access the data is employed through the access control mechanism. Thus, authentication and access control are essential for preserving privacy and securing the fog computing mechanism.[44]

Intrusion detection: The security of every system with quality of service is ensured through the intrusion detection mechanism. The security threat of fog computing is eliminated by checking the genuinity of all incoming data traffic through an intrusion detection system.[45]

Evaluation criteria: The evaluation of the conventional methods is analyzed based on the database utilized for evaluating the performance of the model (E1), evaluation tool utilized for simulating the outcome (E2), evaluation measures utilized for depicting the superiority of the model (E3), analysis of the methods based on formal and informal security analysis (E4). Besides, the type of attack handled by the methods (E5) is also evaluated for all the conventional methods.

5.1.1 | Authentication mechanisms

The approaches developed to ensure the security of fog computing networks based on authentication schemes are detailed in this section. A lightweight authentication technique (E6) for fog computing was designed by[46] using the failover authentication model. This considers the information transmission to the sink node through the fog node. If the corresponding fog node is absent, it is shared through the fast re-authentication secondary node. Registration of the sink node and a fog node enrollment were employed before the authentication phase. Besides, the pre-agreement among the inter-fog nodes was employed before the re-authentication. The analysis based on real or random was employed for the formal security, and informal analysis based on the attacks was performed to depict the resilience of a model.

Multitier broker-based message queue telemetry transport (MQTT) (E6) was designed by,[47] in which lightweight authentication was introduced. The broker was designed at the authentication manager using simple XOR and hash functions. The security threats were eliminated through registration and authentication strategies. The session keys were utilized to perform mutual authentication. Besides, the flow control was accomplished through the authentication manager by handling the requests independently. The analysis depicts the data confidentiality that ensures secure information sharing.

The privacy preservation for the fog computing scenario through identity authentication was designed by[48] for the Internet of Vehicles (IoV). In this, the security elliptic curve-based authentication (E6) was introduced to acquire communication security. The network stability was elevated by selecting the fog head with enhanced behavioral consistency. In addition, reliable communication was accomplished through two-way authentication. The simpler authentication with minimal equipment was accomplished using a roadside unit (RSU) for authentication and trusted authority. In addition, deep learning-based vehicle monitoring ensures the security of a model by preventing illegal vehicles.

Trust-based privacy preservation through signature verification was devised by Soleymani et al.,[49] in which identity verification was ensured through various stages of an authentication process along with the trust measure. The signature verification process before the information sharing ensures the integrity of a model. In addition, the size reduction of a signature eliminates the computation burden, and hence the processing capability based on the computation time was also minimized. Here, the legitimacy of incoming data traffic was performed through the bilinear pairing that assures the integrity of a model.

The digital signature with the decentralized authentication model was designed by Ngabo et al.[50] through security countermeasures. The immutable security was accomplished through the hashing-based signature verification algorithm. The scalability, centralization and latency issues were solved by incorporating the permissioned Blockchain in a fog computing model. In addition, the issues regarding latency were solved through the decentralized model design. Thus, the devised model accomplished a minimal delay with optimal security that guarantees secure information access.

Authentication with signature verification through the zero-knowledge proof was devised by Li et al.[51] to prevent the unauthorized data threat. Besides, an encryption approach was incorporated to preserve the key's privacy. The introduced method isolated the information leakage by offering collision tolerance criteria. The method's computation and communication overhead were minimized by removing redundant information while training the deep learning model. The analysis against malicious users in terms of authentication offers enhanced security.

The authentication approach for fog computing with five levels of security was designed by Eddine et al.[52] through the decentralized architecture. The secrecy of data forwarding, non-repudiation, anonymity, privacy, authenticity, integrity and confidentiality was accomplished by incorporating Blockchain, hashing-based cryptography. The designed model was robust against various attacking strategies and analyzed performance based on security analysis methods. The method minimizes the response time by locating the fog node near the proximity to the vehicles in a network.

The Blockchain-based authentication approach was designed by Zhang et al.[53] to preserve the participant's privacy by removing malicious users. The authentication method was evaluated based on the user credentials; hence, the participants who passed the authentication were allowed to access the information. Besides, the key management schemes assured the reliability of a designed model. Here, the generation of fake queries was employed to confuse the attacker and safeguard a user query's privacy. The limited storage was utilized efficiently through optimal resource allocation.

The optimal secure information sharing in fog computing was designed by Khan et al.[54] with blockchain technique. Enhanced data management was accomplished through optimal data scheduling and balanced resource utilization. A detailed description of related works is provided in Table 1. Here, the security analysis methods are categorized into formal and informal techniques. The security analysis based on the proof of an introduced model constitutes the formal security analysis. In contrast, the discussion regarding the security of an introduced model based on various attacks constitutes the informal security analysis.

Thus, the analysis based on the authentication-based secure data sharing in the fog computing environment has accomplished security through various authentication techniques. The analysis based on various assessment measures such as accuracy, execution time and complexity depicts the model's superiority. Still, the higher computational complexity, cost and execution time limit the model's performance. In addition, the failure to consider the significant attributes that help to prevent un-authenticated access causes performance degradation. Thus, a novel authentication mechanism in the future should solve the above-mentioned issues through efficient attribute consideration and minimizing computation and time complexity.

5.1.2 | Access control mechanisms

The access control mechanism for offering secure and privacy-preserved information sharing in fog computing is detailed in this section. The access control mechanism based on the outsourced scenario was introduced by Zhang et al.[55] to ensure the information correctness processed through the fog layer. In this, the outsourced encryption was utilized to provide the information cryptography and the concrete verification was utilized to verify the user's authentication. Here, the access control mechanism based on the verification criteria diminishes the information leakage and assures information security.

Privacy preservation using the decentralized architecture was designed by Liu et al.[56] for the secure sharing of IoT data. In this, mixed linear and nonlinear spatiotemporal chaotic systems (MLNCML) was utilized for mapping the data. The distributed architecture eliminates single-point failure, and the encryption mechanism enhances information-sharing

TABLE 1 Description of related works.

Reference	Method	Objective	E2	E3	E4	E5	Advantages	Disadvantages
46	Failover Authentication with ECC cryptography	Secure information sharing in IoT with minimal computation complexity	MIRACL library	Execution time, computation cost, communication cost	Analyzed both informal and formal security analysis	Replay, impersonation and man in the middle	Accomplished better performance in terms of functionality and security features.	Failed to analyze the model in a real-time testbed
47	Lightweight authentication with ECC cryptography	Authentication management	OMNeT++ 5.6.2 t	Computation cost, storage overhead	Informal security analysis	Replay, impersonation, and Eavesdropping	Enhanced security with secure and scalable features.	Lack of anonymity and intractability.
48	Identity-based authentication with ECC cryptography	Secure communication between the devices	SUMO	Power consumption	Informal security analysis	Replay, Masquerade, Man-in-the-middle and Sybil	The model ensured privacy protection and vehicle safety.	The computation complexity of a model was higher.
49	Lightweight authentication with ECC cryptography	To accomplish secure and privacy-preserving information sharing in VANET	None	Packet loss ratio, transmission delay, false-positive rate and accuracy	Trust model analysis	Replay, On-and-Off, and Man-in-the-Middle	The devised model can be utilized for real-time application domains due to enhanced security.	The computation and communication cost of a model was higher.
50	Blockchain-based authentication approach with ECC-DSA cryptography	Secure medical data sharing	None	Data retrieval size, latency and standard deviation	None	Social attack	The time utilized for generating the key to ensure security was minimal.	The security of a model was not analyzed and compared.
51	Distributed deep learning with threshold Paillier encryption	To accomplish secure and privacy-preserved information sharing	Java 1.7.0.	Accuracy, running time and transmitted data.	Informal security analysis	Adaptive-chosen-message	The method accomplished balanced functionality, security and efficiency.	The computation overhead exists with a larger number of users.
52	Blockchain-based authentication approach with ECC cryptography	Efficient authentication against cyber attacks	C++	Storage cost, communication and computation complexity.	Analyzed both informal and formal security analysis	DDoS, replay, man-in-the-middle, identity theft, traffic analysis, masquerading, and session key disclosure	The model applied to the Internet of vehicles.	The accuracy of detection was not performed.
53	Blockchain-based authentication approach with biometric encryption	Authentication with privacy preservation and reliable communication	Go 1.13 x64	Average execution time	Informal security analysis	Collision attack	The method accomplished higher efficiency.	The method failed to consider some significant factor like location or attribute that limits the usage of a devised model in some application domains.
54	Blockchain-based authentication approach with SHA-256 encryption	Secure information sharing among UAV	None	Computation cost	None	Not given	Accomplished efficient data management	The comparisons were not performed to depict the superiority of a model

security. Here, the attribute-based access control mechanism assures information availability, integrity and confidentiality. In addition, the smart contract-based access control provides secure information sharing by avoiding single-point failure.

Security assertion mark-up language (SAML) protocol was devised by Rupa et al.[57] to protect the information processing by fog devices. Here, authentication management, along with identity management, ensures access control to mitigate malicious attacks. The access control based on attribute encryption was designed by Olakanmi and Odeyemi[58] to overcome privacy and security issues in the fog computing environment. The two-level security processing with a symmetric key encryption strategy accomplished the fine-grained access control mechanism (FEACS); here, secure health-care information sharing was utilized to analyze a model's performance.

The access control among the fog devices based on secret key establishment and authentication was detailed by Bera et al.,[59] along with certificate verification. The secret credentials are provided after the registration process to accomplish access control. Here, secure communication was ensured through the distributed design of fog servers. The prediction of the attacker is employed through the support vector machine (SVM) based machine learning criteria. The poisoning attack was identified and mitigated through the developed access control mechanism. Besides, the attribute-based encryption for access control was designed by Sun et al.[60] with the decentralized infrastructure. A detailed description of the conventional access control methods is provided in Table 2.

The access control-based security analysis of fog computing depicts secure information sharing with minimal computation complexity through the lightweight mechanism. However, the compromise of a local key is possible and hence limits the security of a model. Thus, designing a novel technique with improved security in the future needs to be accomplished through an efficient key generation strategy. Correspondingly, the computational complexity of a model should be kept minimal for the efficient access control mechanism.

5.1.3 | Authentication and access control mechanisms

The security of fog computing with the combined authentication and access control mechanisms is detailed in this section. A blockchain-based approach which supports identity verification and safeguards communication among edge devices were devised by[61] as a distributed access control and authentication mechanism for the small-scale IoT. The presented approach surpasses a smart contracts authentication scheme compared to the conventional methodology, which a fog computing environment and the concept of a blockchain system have driven. Utilizing the Ethereum approach, registration and authorization mechanism of the user is accomplished. The created method combines authentication mechanisms with the inherent benefits of distributed ledger technology. The distributed ledgers strategy, structure, and layout also offer provenance, consistency, transparency, and data tamper-proof of users.

A security-focused user verification method without considering an authorized user was developed by[62] to manage the devices in a network. The advantages of fog sensor distribution were used in the identity verification scheme without relying on third parties; the verification system provides trustworthy verification between the data owner and requester. The single point of breakdown issues in the backup devices was successfully resolved by the suggested authentication approach employing fog nodes, which also offers several advantages by improving throughput and decreasing cost. The plan considers several agents, including smart contracts, fog nodes, IoT devices, and end devices that assist in administering identification and providing access permissions.

The puncturable encryption (PE) approach was included in the attribute-based matchmaking encryption (AB-ME) method to create the novel authentication approach named fine-grained puncturable matchmaking encryption (FP-ME) was described by Sun et al.[63] Implementing the introduced model assures the validity of the clients' requests, and fulfilling their deadlines was devised instantly using the encryption technique. Delivering a user request within the specified deadline in the authenticated format through the newly designed encryption criteria assures the privacy preservation of a fog computing environment. Network users select the strategy which was available publicly and validated to authenticate the information. Thus, the authenticated strategy was adopted by carriers for encrypting or signing it by utilizing their data as a key. Here, the user considers the perfect companion as described by a strategy based on the particular moment that was decrypted and identified the own information. In this, the analysis of a suggested model depicts that the model was more secure against the adversarial models.

TABLE 2 Description of the conventional access control methods.

Reference	Method	Objective	E2	E3	E4	E5	Advantages	Disadvantages
55	Ciphertext-Policy Attribute-Based Encryption (CP-ABE)	To accomplish the data confidentiality	PYTHON	Key generation time, decryption time	Informal security analysis	Not Given	The attribute encryption-based fine-grained access control minimizes the computation and communication overhead.	The local key compromise is possible and hence limits the security of a model.
56	MLNCML with LSB based encryption	To accomplish secure data sharing	MATLAB	Bit error rate	Informal security analysis	Modification attack	The issue concerning the single-point failure was tackled by the devised approach utilizing the alliance chains.	The computational complexity of a method was higher.
57	SAML Protocol with Ciphertext-Policy Attribute-Based Encryption	To secure the user's identity and information confidentiality	None	Latency, computation overhead, response time and attack rate	None	Various known attacks	The authenticated and privacy-preserved model isolates the attackers through anomaly detection and flow control.	The resource consumption of a model was higher.
58	FEACS with Ciphertext-Attribu Based Encryption	To secure health-care information access from attack	None	Computation and communication cost, signature cost, and encryption and decryption cost.	Formal security analysis	Eavesdropping and inside attack	The complexity of a model was lower due to the lightweight mechanism.	The middle-security issues were not considered while analyzing the security of a model.
59	AI-based access control with SVM based user verification	Secure access control for the Internet of everything.	Node.js language with VS CODE 2019	Computation time	None	Man-in-the-middle, replay, node impersonation, privileged, and insider	Secure data sharing with a correct prediction of an attacker.	The security of the devised model was not analyzed.
60	Distributed IPFS with Decision Bilinear Diffie-Hellman	Secure storage and information updation mechanism	None	Computation cost, and storage cost	Formal security analysis	Keyword attack	Enhanced security was accomplished through the efficient key generation approach.	Elevated storage cost.

A distributed fog environment with the equipment-to-equipment authentication mechanism devised by Patwary et al.[64] was safe by using smart contracts among fog nodes. In this, the security among the equipment was employed through the smart contract. The fog devices enrollment, identification, verification, and information management of the designed model were explored using the Ethereum smart contract. The system model of a designed model comprises different users with their associated activities and participant-to-participant communication exchange. The newly designed model was validated by evaluating the developed and conventional frameworks. The outcomes demonstrated that the suggested model was effective and secure in authenticating and authorizing the information. The suggested technique is secured based on a decentralized manner with minimal overhead concerning the computation cost while analyzing the outcome. A detailed description of reviewed articles with authentication and access control mechanisms is provided in Table 3.

The analysis of secure data sharing in the fog computing environment through the authentication and access control mechanism depicts enhanced security through formal and informal secure analysis. Here, the most challenging aspects that limit the conventional techniques are its higher computation overhead, failure to provide security to all attribute levels of the model, and several other attributes. Hence, a novel technique is essential to solving the issues mentioned above in the future through lightweight authentication and access control mechanisms with enhanced security features.

5.1.4 | Intrusion detection mechanisms

Communication among the fog devices uses several tools and gateways for efficient information sharing with minimal resource utilization, delay and secure transmission. Detection of intrusion in the network model is crucial to provide service quality. Due to the promising solutions, many researchers widely utilize the intrusion detection mechanism based on deep learning. Deep learning-based methods were devised by Sadaf and Sultana.[65] and Abdel-Basset[66] The deep learning-based approach to effectively detect intrusion in the network was designed by Sadaf and Sultana[65] for secure data sharing in fog computing. The method was devised to detect intrusion from normal data traffic in real-time processing. A neural network and unsupervised machine learning methods were integrated into the detection process to improve detection accuracy. The reconstruction loss-based learning strategy assists the developed model in detecting the intrusion for normal data traffic more accurately. A forensic-based deep learning approach was designed by Abdel-Basset[66] for the fog environment. Here, the information loss during the learning stage was eliminated by incorporating the residual connections between the attention layers of a deep learning model. The local attributes were extracted using the recurrent gated unit, and the long-term dependencies were utilized to capture the global representations. Thus, the detection accuracy was elevated along with minimal execution time through the parallel processing of a model. Besides, the distributed learning strategy assists in reducing the challenges faced by centralized learning.

The hybrid deep learning methods for detecting intrusions in the fog computing paradigm are developed by De Souza et al.,[67] Pacheco et al.,[68] Ullah et al.,[69] and Afolabi and Aburas[70] The hybrid deep learning deep neural network-K-nearest neighbor (DNN-KNN) approach was devised by De Souza et al.[67] to detect intrusion in a fog computing layer. Here, the DoS attack was identified for the incoming traffic by considering the attributes like gain ratio, gain information and entropy. The hybrid deep learning model was designed by integrating the k-nearest neighbor and deep neural network to enhance intrusion detection accuracy. The instability of a model was eliminated through hybrid learning, which diminishes the processing overhead and accomplishes minimal memory. Anomaly detection using deep adaptive learning was introduced by[68] to protect the information against attack. The attribute extraction was accomplished using the node's profile-based criteria for predicting the attack. The elevated resiliency of a model assures a more accurate detection rate with minimal false alerts. The analysis based on factors like CPU usage, memory consumption, and computation overhead depicts the minimal processing overhead of a devised model. Hybrid deep learning was devised by[69] for cyber threat detection in the fog environment. The long short-term memory (LSTM) and the convolutional neural network (CNN) was integrated to improve detection accuracy. The analysis shows that the devised model has minimal computation overhead and applies to real data processing. Besides, the developed model performs well for the centralized control mechanism and detects various attack classes. Back propagation-based deep learning was designed by Afolabi and Aburas[70] for prediction intrusion in a fog computing layer. The concept of backpropagation assists in adjusting a neuron's weights by

TABLE 3 Short description of reviewed articles with authentication and access control mechanisms.

Reference	Method	Objective	E2	E3	E4	E5	Advantages	Disadvantages
61	Lightweight approach with smart contract based access control	End-to-end secure communication among mobile devices	None	Time complexity	None		The cost of a model design was minimal due to the consideration of a lightweight mechanism.	The chance of malfunction exists due to the decentralized model design.
62	Hashing based authentication and smart contract based access control	Based on the access control policy, the information was authenticated.	PYTHON	Packet delivery ratio, time and memory	None	Common attacks	Enhanced throughput was accomplished with minimal cost.	Failed to evaluate the performance with a real test bed.
63	FP-ME-based approach	Secure information sharing in real-time among vehicles.	Intellij IDEA2018.2.5 and Java 8	Storage cost and runtime	Performed both informal and formal security analysis	Chosen plaintext and forgery	A fine-grained authentication process accomplished enhanced privacy.	Attribute level privacy was not accomplished.
64	Digital signed authentication with blockchain validation	To accomplish location-based authentication.	None	Elapsed time, and execution cost	Performed both informal and formal security analysis	Secret key guessing and Man-in-the-middle	Accomplished enhanced security through mutual authentication	Higher computation overhead.

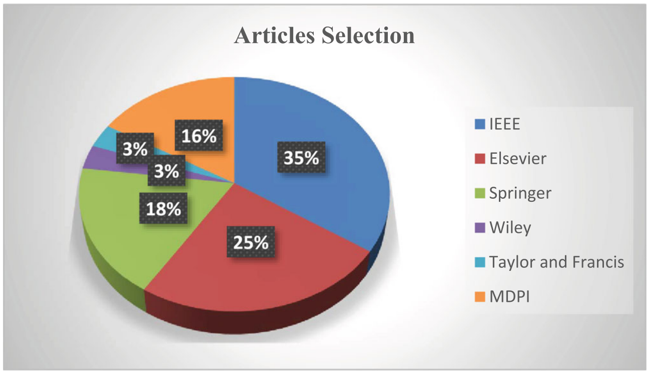

FIGURE 5 Analysis based on review article selection.

estimating the error. The weights were adjusted to enhance the convergence rate to acquire the global solution in predicting fog-layer intrusion. The accuracy of detection was analyzed with various attacks to illustrate the robustness of a model.

The optimized deep learning methods are introduced by Ramkumar et al.,[71] Abdussami,[72] and Abdussami and Farooqui[73] Optimized ensemble learning-based intrusion detection devised by Ramkumar et al.[71] utilized an optimal learning strategy for the fog computing environment. In this, for the incoming data traffic, data transformation was employed to shrink the data, and then, the essential attributes were selected through the filtering approach. The intrusion detection was performed based on the selected attributes by an ensemble classifier. Here, the adjustable parameters of a classifier were modified using the optimization algorithm to elevate the model's detection accuracy. An optimized incremental deep learning method was devised by Abdussami[72] for the fog computing paradigm to ensure the security of information sharing. The essential attributes were extracted from the normalized input data packet before the intrusion detection. Here, minimal error-based incremental learning was employed to improve detection accuracy. Incremental learning-based deep learning was introduced by Abdussami and Farooqui[73] with the optimal feature selection criteria. The temporal and contextual features were extracted from the input data packet. Then, the optimal attribute selection was employed through the hybrid optimization algorithm to minimize irrelevant features based on the correlation estimation. Finally, based on the selected attributes, intrusion detection was devised by the deep learning technique. Here, the additional incremental learning concept was utilized for updating the weights by estimating the error threshold. Table 4 details the short detailed analysis of reviewed methods.

The security analysis through the intrusion detection-based mechanism offers enhanced security through deep learning mechanisms. Nowadays, deep learning mechanism offers promising outcome through the learning criteria. Still, the inefficiency in handling the multitasking capability and the attribute consideration limits the model's performance. Thus, there is a need for a novel technique that enhances security by considering the relevant attributes for enhancing detection accuracy.

6 | ANALYSIS OF METHODS

This section portrayed the analysis of reviewed security analysis articles. The analysis is based on techniques to provide security of the fog computing environment, the database utilized for evaluating the performance, and review documents selection based on publications and year.

6.1 | Analysis based on articles selection sources

The research articles on fog computing security and privacy preservation techniques are selected from various publications and online sources. The detailed analysis is depicted in Figure 5. Most articles from the IEEE journal are selected for the analysis of a proposed security analysis study which 35% of articles chosen from IEEE publications, followed by Elsevier with 25% articles, Springer with 18% research articles, MDPI with 16%, and Taylor & Francis and Wiley with 3% articles each. In addition, a few research articles are chosen from the ACM library, book publications, and several other publications from online sources.

TABLE 4 Short detailed review.

Reference	Method	Objective	E1	E2	E3	E5	Advantages	Disadvantages
67	DNN-KNN	To classify the attacks to identify the malicious nodes for a secure fog computing environment	NSL-KDD and CICIDS2017	None	ACC, Error, Precision, Recall, TNR, F-score, and MCC	Attempted attack	Accomplished superior performance based on performance metrics.	Failed to consider the significant attributes that elevate the accuracy of detection.
65	Autoencoder and Isolation Forest	Securing functioning without compromising the efficiency	KDD CUP99 and NSL-KDD	PYTHON	Accuracy, precision, recall, and F-measure	Unknown attack	Acquired enhanced accuracy in detecting the attacker's device.	The reconstruction loss of a model was higher.
66	Forensics-based DL model (Deep-IFS)	To identify intrusion in the IIoT	BoT-IoT dataset and UNSW-NB15 dataset	Keras Library and TensorFlow API	Accuracy, precision, recall, and F1-measure	Theft, reconnaissance, DDoS, DoS, and legitimate	The recognition time of a model was minimal, and hence the communication cost was reduced.	Failed to recognize the unlabelled attack.
71	Optimized Ensemble learning with Rider Neural Network (RideNN), Deep Neuro Fuzzy Network (DNFN) and Shepard CNN	To discover the intrusion in a fog computing environment	NSL-KDD99 and BOT-IoT dataset	MATLAB	F-measure, precision, recall, and accuracy	Known attacks	The response time of a model was minimal, and privacy, as well as security, were ensured through the analysis.	Failed to extract the appropriate features that enhance the accuracy of detection.
68	Artificial NN (ANN) based deep learning	To analyze the anomaly behavior of a network	None	None	Accuracy, precision, and recall	DDoS	Assures the resiliency and availability of fog computing applications.	The complexity of a model was not analyzed.
72	Modified Electric Fish Optimization-based DNN with Incremental learning	Detects the attack by considering the data attributes	TON_IoT Datasets	MATLAB	Accuracy, sensitivity, precision, specificity, FPR, FNR, FDR, F1-score, MCC, and NPV.		The superiority of a method was portrayed based on the convergence analysis.	Failed to validate the performance.
69	Hybrid CNN + LSTM	Detection of new attacks and threats to manage real-time data.	Coburg Intrusion Detection Data Set (CIDDS-001)	None	Accuracy, precision, recall, and F1-score	Cyber attacks	Cost-effective and flexible to operate.	Failed to identify the newly evolved attacks.
70	Back propagation deep NN (BP-DNN)	To identify the attacks to acquire privacy and secure information sharing.	CIC2017	Jupiter Notebook version 6.1.5	Accuracy	Web attack, Brute Force, DDoS, DoS, FTP, Brute Force SSH, Heartbleed, Infiltration and Botnet	The prediction accuracy was higher, and the computation overhead was minimal compared to conventional methods.	The devised method did not apply to the real-time processing
73	Modified Active Electrolocation-based Electric Fish Optimization based Incremental DNN	To enhance the efficiency of fog computing with secure information sharing by identifying network intrusion.	BoT-IoT dataset	MATLAB	Accuracy, sensitivity, specificity, precision, negative predictive value (NPV), F1Score and Mathews correlation coefficient (MCC)	DDoS	The accuracy of detection was higher due to the optimized learning criteria.	The method was insignificant to handle the attack based on a multitasking environment.

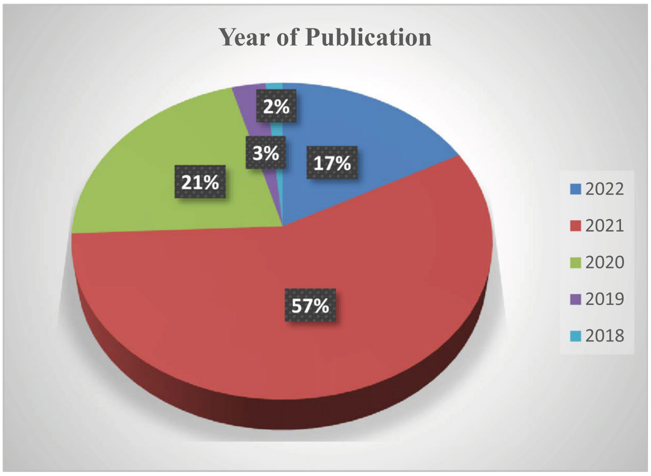

FIGURE 6 Analysis based on publication year of articles.

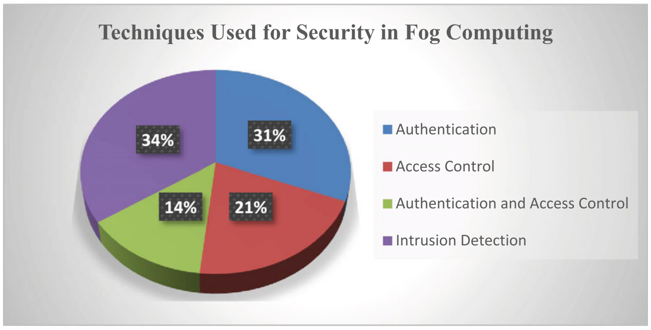

FIGURE 7 Analysis based on techniques used.

6.2 | Year of Publication

The research articles for the study of security in fog computing are chosen from the last five years of publications (2018–2022), as shown in Figure 6. Most articles for the study are chosen from 2021, with 57% of articles, followed by 21% from 2020, 17% from 2022, 3% from 2019 and 2% from 2018 publication years.

6.3 | Techniques Used

The analysis of techniques to provide the security and privacy of information sharing in the fog computing scenario is depicted in Figure 7. While analyzing the security concerns in fog computing, most researchers utilized intrusion detection mechanisms to provide network security. Among the reviewed article, 34% of the researchers utilized the intrusion detection mechanism. Secondly, 31% of reviewed research articles use the authentication approach, and 21% of researcher utilizes access control mechanisms. Finally, 21% of research articles use the authentication and access control mechanism to provide security and privacy when sharing information in a fog computing environment.

6.4 | Dataset Utilized of Analysis

The analysis based on the dataset used to evaluate the performance of a secure data-sharing mechanism is depicted in Figure 8. Most research articles used the IoT-based dataset to analyze the performance; 31% of the researchers used

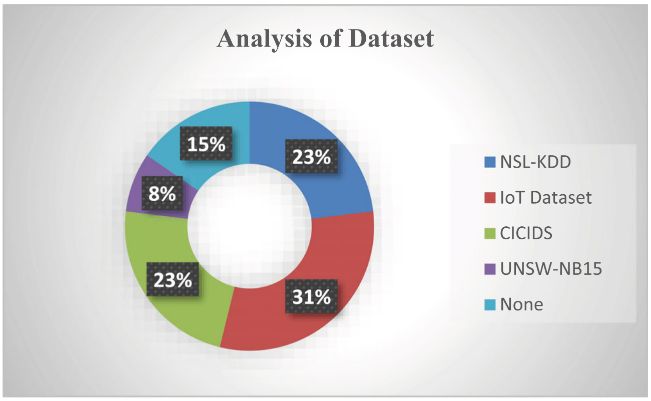

FIGURE 8 Analysis based on Dataset.

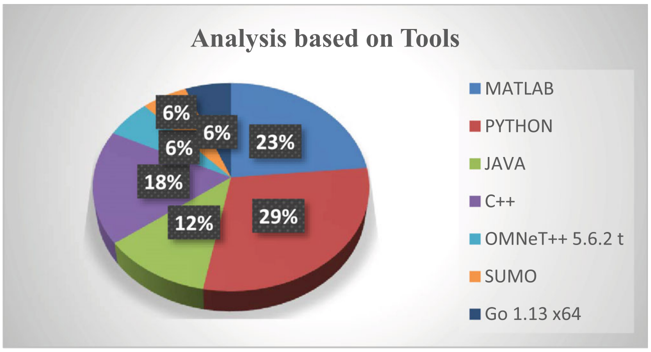

FIGURE 9 Analysis based on Simulation Tools.

IoT-based data. The NSL-KDD and CICIDS data is followed by 23% of the research article. About 15% of the research articles failed to enclose the dataset details utilized to evaluate security model performance.

6.5 | Analysis based on simulation tools

The analysis based on simulation tools is depicted in Figure 9. The simulation models help to verify and interpret the solution accomplished by the introduced research. Hence, the appropriate tool selection is essential to interpret the outcome and evaluate the performance. In most articles, around 29% utilized PYTHON to evaluate the performance. Next, MATLAB is used by 23% of articles, C++ by 18%, JAVA by 12%, and SUMO, Go 1.13x64, and OMNet++5.6.2 t each by 6% of articles.

6.6 | Analysis based on metrics used

The metrics used by the previous researchers to evaluate the security analysis of fog computing are presented in Figure 10. Accuracy measures the closeness of an introduced method with the required target. Thus, accuracy is essential for evaluating the research article's performance, and 21% of researchers evaluate the model's performance. Then, 16% of articles used the execution time analysis, and 4% of research articles used the latency and correlation measure. In addition, various other metrics like packet loss ratio, power consumption, storage cost and several metrics were utilized by research articles to evaluate the performance.

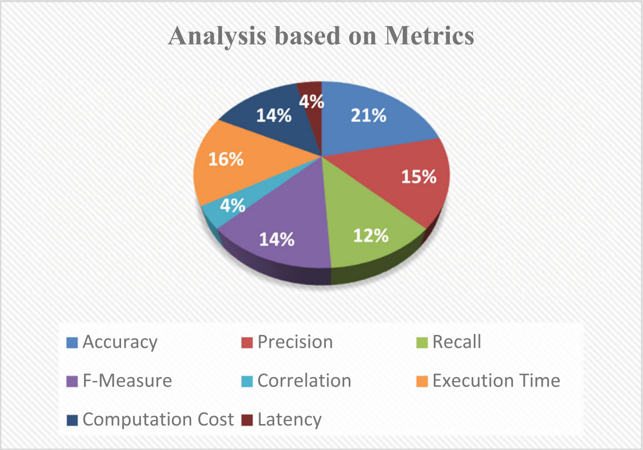

FIGURE 10 Analysis based on Metrics Used.

7 | CHALLENGES IDENTIFIED

The challenges identified by reviewing the conventional security analysis methods of fog computing environments are detailed below.

Trust: A distributed cloud system dealing with trust-related concerns is more challenging for a fog network. While implementing a security framework for a fog network is extremely difficult because of the transparency and two-way trust requirement. However, the cloud has security standards that offer enhanced security, which is still a challenging task for the fog computing environment[11,42–44]

Privacy preservation: Information security is essential to provide information sharing, location and context-aware services for geographically close devices. The sensitive and confidential information sharing utilizes the identity and location of the fog nodes during information processing. Here, the intruder captures the identity and location details as well as captures sensitive information, which makes security more challenging in fog computing.[9,15,20,26,35]

Authentication and key agreement: The role of fog nodes is data gathering and aggregation, in which acquiring authentication with various levels of the gateways creates security issues. Hence, an end-to-end authentication approach and lightweight authentication techniques are considered significant criteria for acquiring secure information sharing in fog computing.[40–49]

Intrusion detection systems: Various attacks in the fog layer are man-in-the-middle attacks, insider attacks, dos attacks, scanning attacks and so on, in which secure information sharing by mitigating the attack is a challenging task. However, security in all the three-tier architecture is essential for safer information sharing.[60–69]

Distributed architecture: The decentralized nature of fog devices makes security issues more challenging because many edge devices utilize the same code for information sharing. Thus, the redundancy of a system model must be minimized to enhance the security of a fog environment[42,45,47–49,51]

Computation hierarchy: The cloud servers are located far from the fog, which generates a trade-off between computation power and response time in information sharing. Fog computing responds to the users, processing the computations and sharing the information with the cloud. Hence, information processing within the specified deadline with minimal computation is a challenging task[54,55,59]

Resource management: In the field of fog computing, various networking and computational resources are dispersed, adaptive and flexible to solve the issues like temporary breakdowns or resource shortages. The resource would not be accessible from the fog node if a fog node failed, the entire system would be unavailable, and the resources are more virtualized. The virtualization of resources generates numerous problems. These difficulties include delay, start-up, positioning, movement of virtual network devices within a fog network, and other related issues[3,19,33,48,52]

Real-world issues: While considering the real time application domains that utilizes the fog computing are the time sensitive fields like the traffic light systems and the health-care system. The response delay due to the DDoS attacks in the network makes the application processing a challenging task[25,38,57]

7.1 | Solutions to overcome the identified challenges

The requirements to overcome the security issues require an efficient technique to eliminate the attack to safeguard the information.

1. Fine-grained access control with lightweight authentication is essential for providing end-to-end authentication with minimal computation overhead. For example, a lightweight authentication with a decentralized framework was designed by Khalid et al.[74] to ensure trusted and legitimate information sharing. Initially, the registration of a system was devised, and then the devise registration was employed based on the smart contract. Lightweight authentication was employed before the communication between the devices using the public keys. The distributed nature and cryptographic properties diminish the model's latency issues. In addition, PoW-based smart verification minimizes energy consumption. The reduced computation and communication costs along with the minimal time complexity, are essential for enhancing the computational speed and security.
2. An intrusion detection mechanism and attack mitigation are essential for detecting and isolating malware from information access to ensure secure information sharing. For example, Deep learning-based anomaly detection, presented by Shakya et al.,[75] introduced attack mitigation for secure data sharing. The functional and spatial information for identifying the anomaly was extracted from the data packet. Network attack detection was employed by the deep neural network, in which host-centric learning was utilized for tuning the model's adjustable parameter. The assessment based on the false alarm and detection rate depicts the scalability and proficiency of a model. Deep learning-based methods are utilized nowadays to enhance the overall performance of a fog computing framework.
3. For processing the real world application domains, the security related methods needs to be tested on the real time test bed environment. Also, the lightweight mechanisms are crucial for the real-time application processing for reducing the computation burden and to meet the demands of the user with minimal latency. The factor like enhanced QoS, low latency, and the location awareness are essential for real time application processing of fog computing paradigm.

The novel security model for fog computing based on the requirement mentioned above ensures enhanced security with minimal computation complexity and enhanced detection accuracy due to the consideration of optimal deep learning technique-based intrusion detection. Also, by considering the significant attributes based on fine-tuning, the authentication and access control mechanism minimizes the computation overhead and enhances security through the efficient authentication process.

8 | FUTURE SCOPE

Security issues: The size enhancement of a geo-distribution network elevates security issues. The malicious attacker targets the application network to attack the information due to the simpler access criteria of a fog device. The authentication approach is utilized for safeguarding the network locally when the server is down. In addition, authentication using conventional public keys is not inefficient due to the scalable infrastructure. Thus, the authentication and access control mechanism is essential for fog computing to accomplish secure information sharing and processing. Hence, the security of a model is assured by providing the appropriate authentication.[45,47,58,65]

Privacy issues: The fog nodes are located close to the end-users; thus, the information contained in the fog nodes is closely related to the user's sensitive information. Hence, secure information sharing is more challenging, generating privacy issues concerning the trust between end users. Thus, the appropriate encryption technique before information sharing is essential for preserving the privacy of information. While handling multiple application domains by the fog device, privacy preservation between the application domains is an essential criterion[58,66,67]

The behavior of nodes: The behavior of fog node analysis helps to identify network intrusion. Still, intrusion detection based on node behavior is not widely analyzed by researchers. Thus, intrusion detection using the behavior of a network is essential by considering the normal and abnormal behavior of the fog nodes for safer communication.[59]

Trustworthy issues: Information processing in the fog computing environment performs several functionalities like data storage, access and computing based on trustworthy consideration. For trustworthy data sharing, secure communication is established between the cloud and edge devices to support network services. The processing of diverse services affects network security, which can be further enhanced through composite services[42,44,57]

9 | CONCLUSION

With the introduction of the IoT, CPS, and mobile Internet, fog computing became a dynamic protocol and popular among researchers. Fog computing is not considered a replacement for cloud computing; it even utilizes the virtualized fabric. In addition, fog computing extends from the outer reaches of information processing to final storage. The data may be kept in the cloud or the user's data center. The proposed analysis of fog computing research details the architecture, layered structure, security and privacy issues, and detailed conventional techniques devised by researchers to overcome security and privacy issues. Moreover, the challenges identified and the future scope to enhance the secure information processing of a fog network is elaborated. Future service enhancements could be made more securely for processing the information by a fog system, which can make superior decisions. In addition, the fog computing network layer still faces the challenge of verifying whether all security measures will operate on limited devices like IoT platforms without developing a fully integrated protection system. Including more gadgets makes security and privacy issues more challenging; hence, security must be ensured at every stage. The decentralized technique's deep learning mechanisms must focus on acquiring better security solutions. In addition, the traffic handling issues are not considered in the proposed security analysis; in the future, without compromising the security and privacy issues, the dynamic workload management will be analyzed for the efficient performance of the model.

FUNDING INFORMATION

No funders were contributed for the preparation of manuscript.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

ORCID

Kamal Kumar Gola https://orcid.org/0000-0001-7018-5192

REFERENCES

1. Ali B, Gregory MA, Li S. Multi-access edge computing architecture, data security and privacy: a review. *IEEE Access*. 2021;9:18706-18721.
2. Memos VA, Psannis KE, Goudos SK, Kyriazakos S. An enhanced and secure cloud infrastructure for e-health data transmission. *Wirel Pers Commun*. 2021;117:109-127.
3. Gupta A, Gupta SK. Flying through the secure fog: a complete study on UAV-fog in heterogeneous networks. *Int J Commun Syst*. 2022;35(13):e5237.
4. Kaur M, Aron R. Focalb: fog computing architecture of load balancing for scientific workflow applications. *Journal of Grid Computing*. 2021;19(4):40.
5. Laroui M, Nour B, Moungla H, Cherif MA, Afifi H, Guizani M. Edge and fog computing for IoT: a survey on current research activities & future directions. *Comp Commun*. 2021;180:210-231.
6. Weng CY, Li CT, Chen CL, Lee CC, Deng YY. A lightweight anonymous authentication and secure communication scheme for FOG computing services. *IEEE Access*. 2021;9:145522-145537.
7. Laghari AA, Jumani AK, Laghari RA. Review and state of art of fog computing. *Arch Comput Methods Eng*. 2021;1-3:3631-3643.
8. Kamoun-Abid F, Rekik M, Meddeb-Makhlouf A, Zarai F. Secure architecture for cloud/fog computing based on firewalls and controllers. *Procedia Computer Science*. 2021 Jan;1(192):822-833.
9. Alamer A. Security and privacy-awareness in a software-defined fog computing network for the internet of things. *Opt Switch Network*. 2021;41:100616.
10. Chen WC, Huang YT, Wang SD. Provable secure group key establishment scheme for fog computing. *IEEE Access*. 2021;9:158682-158694.
11. Samann FE, Abdulazeez AM, Askar S. Fog computing based on machine learning: a review. *Int J Interact Mob Technol*. 2021;15(12):21-46.
12. Ahmadi Z, HaghiKashani M, Nikravan M, Mahdipour E. Fog-based healthcare systems: a systematic review. *Multimed Tools Appl*. 2021;80:36361-36400.
13. Erskine SK, Elleithy KM. Real-time detection of DoS attacks in IEEE 802.11 p using fog computing for a secure intelligent vehicular network. *Electronics*. 2019;8(7):776.
14. Mukherjee M, Matam R, Shu L, et al. Security and privacy in fog computing: challenges. *IEEE Access*. 2017;5:19293-19304.
15. Kumar J, Singh AK. Security and privacy-preservation of IoT data in cloud-fog computing environment. arXiv:2212.00321. 2022.

16. Pareek K, Tiwari PK, Bhatnagar V. Fog computing in healthcare: a review. *IOP Conference Series: Materials Science and Engineering*. Vol 1099. IOP Publishing; 2021:12025.
17. Zhang P, Zhou M, Fortino G. Security and trust issues in fog computing: a survey. *Fut Gener Comput Syst*. 2018;88:16-27.
18. Ometov A, Molua OL, Komarov M, Nurmi J. A survey of security in cloud, edge, and fog computing. *Sensors*. 2022;22(3):927.
19. Al-Khafajiy M, Otoum S, Baker T, et al. Intelligent control and security of fog resources in healthcare systems via a cognitive fog model. *ACM Trans Internet Technol*. 2021;21(3):1-23.
20. Ranaweera P, Jurcut AD, Liyanage M. Survey on multi-access edge computing security and privacy. *IEEE Commun Surv Tutor*. 2021;23(2):1078-1124.
21. Kalyani Y, Collier R. A systematic survey on the role of cloud, fog, and edge computing combination in smart agriculture. *Sensors*. 2021;21(17):5922.
22. Vakilian S, Moravvej SV, Fanian A. Using the artificial bee colony (ABC) algorithm in collaboration with the fog nodes in the internet of things three-layer architecture. *In2021 29th Iranian Conference on Electrical Engineering (ICEE)*. IEEE; 2021:509-513.
23. Rafiq A, Ping W, Min W, Muthanna MS. Fog assisted 6TiSCH tri-layer network architecture for adaptive scheduling and energy-efficient offloading using rank-based Q-learning in smart industries. *IEEE Sens J*. 2021;21(22):25489-25507.
24. Alammari A, Moiz SA, Negi A. Enhanced layered fog architecture for IoT sensing and actuation as a service. *Sci Rep*. 2021;11(1):21693.
25. Ketu S, Mishra PK. Cloud, fog and mist computing in IoT: an indication of emerging opportunities. *IETE Techn Rev*. 2022;39(3):713-724.
26. Alwakeel AM. An overview of fog computing and edge computing security and privacy issues. *Sensors*. 2021;21(24):8226.
27. Agarwal E. *A Review on VANET Security Attacks*. Barak Education Society; 2022:45.
28. Khater BS, Abdul Wahab AW, Idris MY, et al. Classifier performance evaluation for lightweight IDS using fog computing in IoT security. *Electronics*. 2021;10(14):1633.
29. Sharma M, Bhushan B, Khamparia A. Securing internet of things: attacks, countermeasures and open challenges. *Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2020*. Vol 1. Springer; 2021:873-885.
30. Gowda NC, Manvi SS. An efficient authentication scheme for fog computing environment using symmetric cryptographic methods. *2021 IEEE 9th Region 10 Humanitarian Technology Conference (R10-HTC)*. IEEE; 2021:1-6.
31. Ali Z, Chaudhry SA, Mahmood K, Garg S, Lv Z, Zikria YB. A clogging resistant secure authentication scheme for fog computing services. *Comput Netw*. 2021;185:107731.
32. Xie Q, Han J, Ding Z. Provable secure authentication protocol in fog-enabled smart home environment. *Sustainability*. 2022;14(21):14367.
33. Das AK, Kalam S, Sahar N, Sinha D. UCFL: user categorization using fuzzy logic towards PUF based two-phase authentication of fog assisted IoT devices. *Comput Secur*. 2020;97:101938.
34. Borkar GM, Patil LH, Dalgade D, Hutke A. A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: a data mining concept. *Sustain Comput: Inform Syst*. 2019;23:120-135.
35. Raja G, Anbalagan S, Vijayaraghavan G, Dhanasekaran P, Al-Otaibi YD, Bashir AK. Energy-efficient end-to-end security for software-defined vehicular networks. *IEEE Trans Industr Inform*. 2020;17(8):5730-5737.
36. Ferrag MA, Shu L, Djallel H, Choo KK. Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0. *Electronics*. 2021;10(11):1257.
37. Bousselham M, Benamar N, Addaim A. A new security mechanism for vehicular cloud computing using fog computing system. *2019 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)*. IEEE; 2019:1-4.
38. Moqurrab SA, Tariq N, Anjum A, et al. A deep learning-based privacy-preserving model for smart healthcare in internet of medical things using fog computing. *Wirel Person Commun*. 2022;126(3):2379-23401.
39. Krsul I, Spafford E, Tuglular T. A new approach to the specification of general computer security policies. *COAST Tech Rep*. 1998;13-97.
40. Bejtlich R. *Interpreting Network Traffic: A Network Intrusion Detector's Look at Suspicious Events*. 2000.
41. Kuperman GG, Whitaker RD, Brown SM. Cyber warrior: information superiority through advanced multi-sensory command and control technologies. *Proceedings of the IEEE 2000 National Aerospace and Electronics Conference. NAECON 2000. Engineering Tomorrow (Cat. No. 00CH37093)*. IEEE; 2000:263-271.
42. Abdali TA, Hassan R, Aman AH, Nguyen QN. Fog computing advancement: concept, architecture, applications, advantages, and open issues. *IEEE Access*. 2021;9:75961-75980.
43. Kürtünlüoğlu P, Akdik B, Karaarslan E. Security of virtual reality authentication methods in metaverse: an overview. arXiv:2209.06447. 2022.
44. Egala BS, Pradhan AK, Badarla V, Mohanty SP. Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. *IEEE Internet Things J*. 2021;8(14):11717-11731.
45. Khan MA. HCRNNIDS: hybrid convolutional recurrent neural network-based network intrusion detection system. *Processes*. 2021;9(5):834.
46. Banerjee S, Das AK, Chattopadhyay S, Jamal SS, Rodrigues JJ, Park Y. Lightweight failover authentication mechanism for IoT-based fog computing environment. *Electronics*. 2021;10(12):1417.
47. Kurdi H, Thayananthan V. A multitier MQTT architecture with multiple brokers based on fog computing for securing industrial IoT. *Appl Sci*. 2022;12(14):7173.
48. Song L, Sun G, Yu H, Du X, Guizani M. Fbia: a fog-based identity authentication scheme for privacy preservation in internet of vehicles. *IEEE Trans Veh Technol*. 2020;69(5):5403-5415.
49. Soleymani SA, Goudarzi S, Anisi MH, Zareei M, Abdullah AH, Kama N. A security and privacy scheme based on node and message authentication and trust in fog-enabled VANET. *Veh Commun*. 2021;29:100335.

50. Ngabo D, Wang D, Iwendi C, Anajemba JH, Ajao LA, Biamba C. Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things. *Electronics*. 2021;10(17):2110.
51. Li Y, Li H, Xu G, Xiang T, Huang X, Lu R. Toward secure and privacy-preserving distributed deep learning in fog-cloud computing. *IEEE Internet Things J*. 2020;7(12):11460-11472.
52. Eddine MS, Ferrag MA, Friha O, Maglaras L. EASBF: an efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles. *J Inf Secur Appl*. 2021;59:102802.
53. Zhang C, Zhu L, Xu C. BPAF: blockchain-enabled reliable and privacy-preserving authentication for fog-based IoT devices. *IEEE Cons Electron Mag*. 2021;11(2):88-96.
54. Khan AA, Laghari AA, Gadekallu TR, et al. A drone-based data management and optimization using metaheuristic algorithms and blockchain smart contracts in a secure fog environment. *Comput Electr Eng*. 2022;102:108234.
55. Zhang J, Cheng Z, Cheng X, Chen B. OAC-HAS: outsourced access control with hidden access structures in fog-enhanced IoT systems. *Connect Sci*. 2021;33(4):1060-1076.
56. Liu Y, Zhang J, Zhan J. Privacy protection for fog computing and the internet of things data based on blockchain. *Cluster Comput*. 2021;24:1331-1345.
57. Rupa C, Patan R, Al-Turjman F, Mostarda L. Enhancing the access privacy of IDaaS system using SAML protocol in fog computing. *IEEE Access*. 2020;8:168793-168801.
58. Olakanmi O, Odeyemi K. FEACS: a fog enhanced expressible access control scheme with secure services delegation among carers in E-health systems. *Internet Things*. 2020;12:100278.
59. Bera B, Das AK, Obaidat MS, Vijayakumar P, Hsiao KF, Park Y. AI-enabled blockchain-based access control for malicious attacks detection and mitigation in IoE. *IEEE Cons Electron Mag*. 2020;10(5):82-92.
60. Sun J, Yao X, Wang S, Wu Y. Non-repudiation storage and access control scheme of insurance data based on blockchain in IPFS. *IEEE Access*. 2020;8:155145-155155.
61. Joshi S, Stalin S, Shukla PK, et al. Unified authentication and access control for future mobile communication-based lightweight IoT systems using blockchain. *Wirel Commun Mobile Comput*. 2021;2021:1-2.
62. Pallavi KN, Ravi KV. Authentication-based access control and data exchanging mechanism of IoT devices in fog computing environment. *Wirel Person Commun*. 2021;116:3039-3060.
63. Sun J, Xu G, Zhang T, Alazab M, Deng RH. A practical fog-based privacy-preserving online car-hailing service system. *IEEE Trans Inf Forensics Secur*. 2022;17:2862-2877.
64. Patwary AA, Fu A, Battula SK, Naha RK, Garg S, Mahanti A. FogAuthChain: a secure location-based authentication scheme in fog computing environments using blockchain. *Comp Commun*. 2020;162:212-224.
65. Sadaf K, Sultana J. Intrusion detection based on autoencoder and isolation forest in fog computing. *IEEE Access*. 2020;8:167059-167068.
66. Abdel-Basset M, Chang V, Hawash H, Chakrabortty RK, Ryan M. Deep-IFS: intrusion detection approach for industrial internet of things traffic in fog environment. *IEEE Trans Industr Inform*. 2020;17(11):7704-7715.
67. De Souza CA, Westphall CB, Machado RB, Sobral JB, dos Santos VG. Hybrid approach to intrusion detection in fog-based IoT environments. *Comput Netw*. 2020;180:107417.
68. Pacheco J, Benitez VH, Felix-Herran LC, Satam P. Artificial neural networks-based intrusion detection system for internet of things fog nodes. *IEEE Access*. 2020;8:73907-73918.
69. Ullah I, Raza B, Ali S, Abbasi IA, Baseer S, Irshad A. Software defined network enabled fog-to-things hybrid deep learning driven cyber threat detection system. *Secur Commun Netw*. 2021;2021:1-5.
70. Afolabi HA, Aburas A. Proposed back propagation deep neural network for intrusion detection in internet of things fog computing. *Int J*. 2021;9(4):464-469.
71. Ramkumar MP, Daniya T, Paul PM, Rajakumar S. Intrusion detection using optimized ensemble classification in fog computing paradigm. *Knowl-Based Syst*. 2022;252:109364.
72. Abdussami AA. Incremental deep neural network intrusion detection in fog based IoT environment: an optimization assisted framework. *Indian J Comp Sci Eng*. 2021;12(6):1847-1859.
73. Abdussami AA, Farooqui MF. Optimal feature selection with weight optimized deep neural network for incremental learning-based intrusion detection in fog environment. *J Inf Knowl Manag*. 2022;21(3):2250042.
74. Khalid U, Asim M, Baker T, Hung PC, Tariq MA, Rafferty L. A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Clust Comput*. 2020;23(3):2067-2087.
75. Shakya S, Pulchowk LN, Smys S. Anomalies detection in fog computing architectures using deep learning. *J Trends Comput Sci Smart Technol*. 2020;2(1):46-55.

How to cite this article: Gola KK, Arya S, Khan G, Devkar C, Chaurasia N. Security analysis of fog computing environment for ensuring the security and privacy of information. *Trans Emerging Tel Tech*. 2023;34(10):e4861. doi: 10.1002/ett.4861