International Journal of Networked and Distributed Computing (2026) 14:14
https://doi.org/10.1007/s44227-026-00093-4

REVIEW ARTICLE

Fog Computing: A Comprehensive Review on Security Analysis, Attacks, and Future Prospects

Kamal Kumar Gola[1] · Shikha Arya[2] · Gulista Khan[3] · Mridula Singh[4] · Sagar Gulati[5] · Nishant Chaurasia[6] · Rohit Kanauzia[7] · Sumit Kumar[8]

Received: 6 January 2025 / Revised: 29 November 2025 / Accepted: 16 March 2026

Abstract

Fog computing, as an extension of cloud computing to corporate networks, facilitates communication between endpoint devices and data centers for processing, storing, and utilizing network services. With the increasing adoption of cloud storage by individuals and corporations, information security has become a growing concern. This diverse range of capabilities raises security issues related to data, reliability, privacy, and network communication. This paper extensively examines safety concerns and various techniques within fog computing designed to address these challenges. It introduces a technological taxonomy, categorizing fog security concerns and their solutions into three main areas: network service, data processing, and privacy. The study surveys current literature to identify security-focused research approaches and associated fog computing solutions, analyzing them from analytical and statistical perspectives. The document delves into server issues and explores the pros and cons of suggested cloud protection strategies. Drawing on the findings, the paper puts forward proposals to tackle fog computing security issues. Finally, it outlines future research directions aimed at the development, deployment, and maintenance of fog systems, taking into consideration existing challenges.

Keywords Security · Fog computing security · Edge computing · Cloud computing · IoT · Fog attacks · Fog privacy

✉ Kamal Kumar Gola
kkgolaa1503@gmail.com

Shikha Arya
shikha.srms@gmail.com

Gulista Khan
gulista.khan@gmail.com

Mridula Singh
mridulaiitr@gmail.com

Sagar Gulati
sagarg40@gmail.com

Nishant Chaurasia
rgtu.nishant@gmail.com

Rohit Kanauzia
kanauziarohit@gmail.com

Sumit Kumar
mail2dr.sumit@gmail.com

[1] Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun 248002, India

[2] Department of Computer Science and Engineering, Indian Institute of Technology, Roorkee 247667, India

[3] Department of Computer Science and Engineering, Teerthanker Mahaveer University, Moradabad 244001, India

[4] Department of Computer Science and Engineering, Quantum University, Roorkee 247667, India

[5] School of CS and IT, JAIN (Deemed-to-be University), Bengaluru, Karnataka 560069, India

[6] Department of Computer Science and Engineering, Dr B R Ambedkar National Institute of Technology, Jalandhar 144011, India

[7] Department of Computer Science and Engineering, School of Science & Technology, Swami Rama Himalayan University, Dehradun 248016, India

[8] Department of Computer Science and Engineering, Shivalik College of Engineering, Dehradun 248197, India

Published online: 04 April 2026

1 Introduction

The evolution of virtualization as a robust platform has effectively met the increasing demand for processing data from end-users through cloud services and storage [1]. The surge in connecting devices and applications stemming from the Internet of Things (IoT), such as smartphones, gadgets, and Google Glass, has become more pronounced in recent years [2]. This heightened connectivity often leads to congestion when numerous devices are linked to cloud service facilities.

While cloud computing has the potential to enhance various quality-of-service components, including frequency band, confidentiality, latency, capacity, response speed, security, and computation [3, 4], challenges arise when dealing with the congestion caused by the multitude of connected devices. The architecture of fog computing emerges as a promising solution, supporting the IoT principle by facilitating communication and interaction among almost all nodes and devices. This fog computing paradigm holds significant promise for both academia and industry, offering a substantial approach to address the issues mentioned in [5].

Fog computing plays a crucial role in processing data collected from the Internet of Things (IoT), with a focus on minimizing latency through the use of network devices [6]. Within fog environments, the components located at the end of diverse networks are commonly referred to as fog nodes. These nodes encompass local area networks, edge routers, routers, switches, gateways, and a dedicated network cloud [7]. The network cloud facilitates the uniform and efficient management of resources, including networking, storage allocation, and computing [8]. Fog nodes have the capability to construct comprehensive edge devices and frequently handle the associated data in IoT scenarios. The cloud can be integrated seamlessly with existing processes and applications [9]. However, various threat scenarios arise due to the lack of trustworthy technology, especially in programming networks within these clouds, providing potential platforms for attackers. Research on fog computing is ongoing, and numerous tutorials and review papers have been published over the past several years to contribute to the understanding of this evolving field.

Several reports on independent fog computing frameworks and architectures have been published, focusing on various applications within the Internet of Things (IoT) [10–12]. These frameworks often address security features critical for life safety systems [13]. However, the inherent variability, mobility, and extensive geographic distribution of fog present challenges for effective study using current methodologies [14]. Trust and dependability issues in a fog computing environment arise from concerns such as unauthorized access, data breaches, compromised devices, malicious attacks, and overall system integrity. Addressing these challenges necessitates the development of new security approaches tailored specifically to fog computing to mitigate trust-related problems. The existing literature lacks a well-defined categorization of security frameworks and measures for different aspects of the fog environment.

1.1 Scope of this Review

Given the rapid evolution of fog computing and the emergence of new security challenges and solutions, this paper specifically focuses on the security dimension of fog computing. The scope of this review is limited to three major aspects: network security, data security, and privacy preservation in fog environments. To provide clarity and novelty, we establish a taxonomy that not only organizes existing threats and defenses but also identifies gaps in current approaches, including underexplored areas such as insider threats and lightweight cryptography. Unlike earlier surveys (e.g., Singh 2021), this paper positions itself through a taxonomy + gap analysis framework, ensuring researchers and practitioners gain both a structured categorization and clear directions for future work.

1.2 Research Motivation

Cloud computing was introduced as a new informatics paradigm and as the bridge to digital network infrastructure and edge devices or IoT devices. The Cisco service provider created fog computing to support the most users and flexible services with the fewest resources instead of cloud computing. However, during the early phases of its implementation, especially in IoT, several challenges were encountered, including delay, trust, security, attacks, threats, and privacy. Therefore, the primary difficulties of the fog computing paradigm concern privacy. When foggy, the critical computer components are typically adequately evaluated based on every operational criterion, both endpoints and access points. Characteristics like blockchains, artificial intelligence, and SDN are considered to address the security issue in fog computing.

The presented study intends to review the state-of-the-art security issues related to fog computing across network, data, and privacy layers and provide an updated taxonomy that reflects both existing solutions and unexplored gaps. By doing so, it offers valuable insights into ongoing challenges and outlines potential directions for researchers and application developers.

2 Literature Review

Recent studies on fog security highlight diverse approaches but also reveal fragmentation in focus. In [15], the authors provide a taxonomy-driven analysis of fog monitoring challenges, proposing a structured framework to address QoE and SLA concerns. While valuable, this taxonomy remains largely infrastructure-centric, overlooking emerging issues like insider threats. Complementing this [16], emphasizes ecosphere diversification and the role of IDS for detecting DoS/DDoS attacks. Although IDS is widely recognized, its computational cost raises contradictions when applied to resource-constrained fog environments.

Several works examine fog's relationship with cloud and edge. For example [17], explores fog computing's implementation alongside cloud infrastructures, highlighting QoS, security, and bandwidth allocation, while [18] categorizes secure data collection at the cloud layer. These works underscore fog's role in improving performance, yet they provide limited insight into privacy-preserving methods specific to distributed architectures. Similarly [19], and [20] extend this discussion to encryption, authorization, and resource utilization but stop short of addressing lightweight cryptographic methods tailored for fog's constraints.

Beyond general frameworks, some studies propose novel computational and architectural solutions. In [21], security management is approached using Analytic Hierarchy Process (AHP) combined with neutrosophic set theory, offering a rigorous multi-criteria decision-making framework. However, its complexity may hinder adoption in highly dynamic fog environments. In contrast [22], introduces an IDS-based defense against Advanced Persistent Threats in mobile fog systems, leveraging machine learning for detection with notable accuracy, though such solutions still face deployment challenges due to training overhead.

Emerging paradigms integrate blockchain and collaborative intelligence into fog security. For instance [23], proposes a blockchain-based authentication scheme for traffic light systems, demonstrating resilience and low latency. Similarly [24], presents NADA, a machine learning-based architecture for detecting DoS/DDoS attacks, which achieves high accuracy but raises questions of scalability under massive IoT-fog deployments. In the healthcare domain [25], introduces FC-SEEDA, an energy-efficient secure data aggregation scheme for IoHT. While effective in conserving energy and safeguarding sensitive health data, it illustrates the trade-off between computational overhead and security strength.

Taken together, these studies underscore significant progress in authentication, intrusion detection, and blockchain-based security in fog environments. However, critical gaps remain. First, lightweight cryptographic approaches suitable for constrained fog nodes are rarely explored. Second, insider threats and multi-tenant privacy issues are underrepresented in existing taxonomies. Finally, contradictions persist—for example, IDS solutions that improve detection accuracy often conflict with fog's low-latency and low-power requirements. This synthesis indicates the need for future work that balances strong security with fog's inherent limitations, bridging the gap between theoretical models and deployable solutions.

2.1 Main Contributions

The major contributions of this literature review are summarized as follows:

- Provides a structured thematic synthesis of prior research, grouping studies into key fog security domains such as authentication, access control, intrusion detection, privacy-preservation, trust management, and blockchain-based approaches, rather than presenting them as isolated works.
- Establishes a comparative classification system that analyzes security challenges across ten categories: authentications, access control attacks, data distribution, data processing, user privacy, location privacy, trust management, virtualization, detection systems, and packet forwarding.
- Critically evaluates the trade-offs and contradictions identified in the literature (e.g., balancing energy efficiency with latency, or strong encryption with constrained fog resources), offering a clearer understanding of current limitations.
- Identifies research gaps such as insider threats, lightweight cryptography, and homomorphic encryption for fog environments, which remain underexplored in the existing body of work.
- Highlights future research directions by outlining unresolved issues and emerging approaches, thereby guiding researchers toward more fog-specific and scalable security solutions.

2.2 Research Methodology and Evaluation

To fulfill the purpose of this review, the study was structured to respond to the following key research questions:

- What are the critical security challenges faced by fog computing systems, beyond those inherited from cloud environments?
- What are the strengths and weaknesses of existing fog security mechanisms, particularly in addressing

distributed trust, multi-tenant environments, and resource-constrained devices?
- How do current approaches handle privacy concerns (e.g., data confidentiality, location privacy, user identity protection), and what contradictions or trade-offs exist among them?
- Which areas remain insufficiently addressed (e.g., insider threats, lightweight encryption, homomorphic encryption), and what directions should future research pursue?
- Databases searched: IEEE Xplore, ACM DL, SpringerLink, Elsevier, Web of Science.
- Date range: 2015–2025.
- Search strings: "fog computing security," "fog attacks," "fog privacy," "fog authentication," etc.
- Inclusion criteria: peer-reviewed works addressing fog/edge security.
- Exclusion criteria: works focused solely on cloud/edge without fog relevance.
- Screening process: two-phase review (title/abstract screening followed by full-text analysis).

The primary data sources include IEEE Xplore and Web of Science, ensuring broad coverage of peer-reviewed works. Studies were categorized thematically (authentication, privacy, intrusion detection, blockchain-based security, etc.), and compared to highlight contradictions, complementarities, and gaps. This systematic approach ensures that the review moves beyond a descriptive summary and provides a critical synthesis that reflects both the current state and future trajectory of fog security research.

3 Overview of Fog Computing

Cisco Systems introduced the term "fog computing" in 2011, not as a replacement for cloud computing but as a system developed to address gaps in services that occur in close proximity [26]. Unlike the ethereal nature of clouds in the sky, fog generally occurs near the ground. In contrast to the cloud, which serves nearby end-users, fog computing positions itself to offer services close to users, addressing their needs rapidly. However, fog computing has occasional access to resources and provides limited processing capacity. Fog computing is a technique that involves storing and processing model data by concentrating it in hardware near the network's edge, rather than relying solely on the web [27]. In essence, it is a simulated environment that complements cloud computing data centers, where end nodes transmit storage and connectivity resources not explicitly situated at the network's edges, according to Cisco Systems. Various definitions of fog computing exist among academics and institutions, with one of the more general definitions provided by [28].

As stated by its declaration, fog computing is A geographically distributed computing architecture with a resource pool that consists of one or more ubiquitously connected heterogeneous devices at the edge of the network (including edge devices) and is not exclusively seamlessly backed by Cloud services to collaboratively provide elastic computation, storage, and communication (as well as many other new services and tasks) in isolated environments to a large user base. The use of the cloud environment was defined in [29] as a scenario where a large number of heterogeneous (wireless and occasionally autonomous), ubiquitous, and decentralized devices communicate and potentially cooperate among themselves and with the network to perform storage and processing tasks without the involvement of third parties. These responsibilities could include starting new programs and services or staying on top of crucial network activities. Users benefit from renting some of their gear to host these services.

The International Cloud Initiative defines fog computing [30] as a system-level horizontal architecture that distributes resources and services, encompassing processing, storage, control, and networking, from the Cloud to Things. Cloud computing provides efficient services and compact storage across storage systems for edge routers. Edge computing typically relates to location, while fog computing involves deploying storage resources, computation, and service communication on or near devices under the control of end consumers. Fog computing facilitates Internet of Things (IoT) operations by connecting a vast number of devices across the internet. It features advantages such as response time, contextual awareness, mobility support, extensive sensor networks, numerous nodes, real-time interaction, and dominance in wireless access. Various systems, including parking systems, traffic flow, and the healthcare industry, benefit from monitoring and improvement through fog computing. The technology contributes to user-centric data delivery, supports IoT and mobility, reduces network congestion, provides excellent scaling capabilities, allows future cloud integration, and enhances data processing and distribution efficiency.

Despite its numerous benefits, fog computing has significant drawbacks that warrant careful consideration. It introduces network complexity, leading to increased business overhead. Nonetheless, it offers an improved administrative procedure and seamless consumer interaction, constituting a software and electronics system with very low latency for monitoring, controlling, and analyzing data. Additionally, fog computing does not provide lasting capacity, reduces demand on the cloud, and cuts costs by eliminating unnecessary data from its computational storage [31].

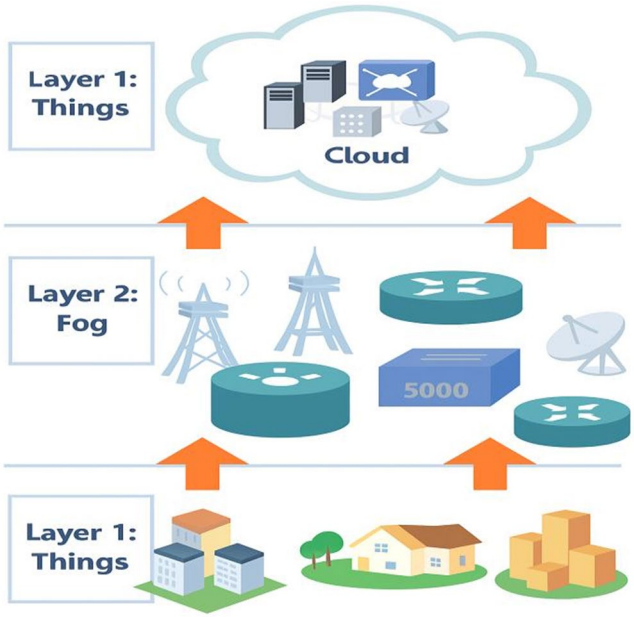

Fig. 1 Three-tier model of fog computing

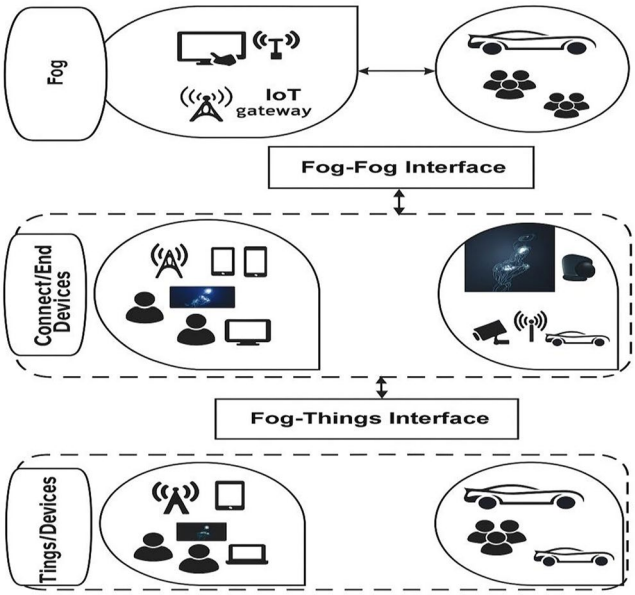

Fig. 2 Cloud applications in the two-tier paradigm of cloud cover tech

3.1 Fog Computing Architecture

The two alternative architectures for fog computing are (I) Cloud-Fog-Device architecture and (II) Fog-Device architecture [35]. The Cloud-Fog-Device structure shown in Fig. 1 is a three-tiered system, while the basic construction of a cloud cover instrument is shown as a two-tier model in Fig. 2.

- The Cloud-Fog-Device architecture has three levels: the design concept cloud, fog computing, and the device. This architecture uses fog to connect the device tier of data-generating resources for processing and storing with the computational cloud resources. Mobile and stationary devices are the two main categories in the device tier [32]. Routers, gateways, bridges, switches, and base computing devices, such as local servers, develop the network hardware in the fog tier. The cloud tier serves as a platform for processing and storage in a three-tier system. Access to the cloud, which has lots of processing and storage capacity, is available worldwide.
- The two-tiered fog-device architecture makes up the construction of fog computing and devices. With this concept, fog nodes coordinate the delivery of a range of services without the interference of cloud servers. In comparison, in a cloud-fog-device architecture, fog nodes investigate and prepare the information obtained by internet devices before routinely providing a data summary to the cloud in line with the internal hierarchical structure. Fog can process, transfer, and store the data from mobile or fixed devices that are a part of the device layer in the two-tier architecture [33]. The tiers are connected via arrange of connection technologies, such as wired connections, broadband connections, or combinations of both [34].

Fog nodes are crucial to the general operation of fog computing because they collect data from many sources for subsequent cleaning. Furthermore, fog computing may be categorized into the following layers: physical and virtualization layer, monitoring layer, pre-processing layer, temporary storage layer, security layer, and transit layer. An illustration of the six-layer architecture of fog computing [35] is provided in Fig. 3.

3.1.1 Physical and Virtualization Layer

This layer contains various virtual networks, sensor networks, and physical structures. Different types of centrally dispersed sensors are employed to monitor the environment and share data they gather to higher levels through channels to be processed and filtered appropriately. Numerous gadgets, such as smart homes, appliances, et al., may produce these data.

3.1.2 Monitoring Layer

This layer monitors and tracks resource usage, sensor and fog node availability, and network components. The component of resource demand checks the available resources and forecasts future resources based on user behavior and usage. Any difficult circumstances where a failure could happen must be resolved. Forecasting monitors according

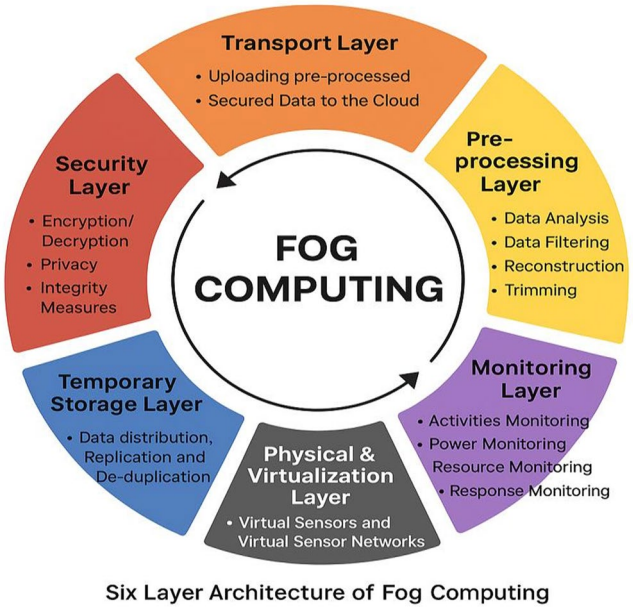

Fig. 3 Six –layer architecture of fog computing

to network load and resource availability to determine fog system performance. In this layer, every task carried out by nodes is monitored, including which node is doing the task at which time and what will be asked of it next. Every program or assistance installed on the infrastructure is updated regarding its state and performance.

3.1.3 Pre-Processing Layer

Within data management, the pre-processing layer plays a crucial role by engaging in tasks such as data analysis, filtering, trimming, and reconstruction. Once meaningful information is extracted through processing, the data can be stored locally in the fog or transferred to the cloud for long-term storage [41]. The core idea behind this approach is to send frequently accessed data to fog servers and less frequently used or archival data to the cloud. Consider an intelligent transportation application that generates data from numerous sensors. While the details are collected and analyzed to generate desired information, not all created data may hold value, making the storage of all such data less than ideal. For instance, a sensor may produce details every second, but based on the application's needs, a measure of the average details over minutes or a specific timeframe is stored. This process involves compressing the details to ensure that the data volume does not become excessively large.

3.1.4 Temporary Storage Layer

Data backup is performed to avert data loss and guarantee data accessibility. The pre-processed data are briefly kept inside the covering of the storage device. To manage storage across a network and operate as a single storage device, a group of hardware components is used for the concept of storage virtualization. This hardware component is easy to use and maintains this personal storage box. The main benefit of storage virtualization is increasing business functionality while lowering hardware and storage expenses, which also lessens the storage complexity.

3.1.5 Security Layer

The security layer in fog computing plays a critical role in ensuring confidentiality, integrity, and trust across distributed nodes. While traditional encryption techniques such as symmetric and asymmetric cryptography provide a baseline, they are insufficient for the unique challenges of fog environments, which involve distributed trust, multitenancy, and resource-constrained devices. To address these issues, recent advancements emphasize fog-specific solutions such as **homomorphic encryption**, which enables computation on encrypted data without decryption, thereby preserving privacy during processing on untrusted nodes. **Lightweight blockchain-based authentication** provides decentralized, tamper-resistant identity management and auditability while avoiding single points of failure. Similarly, **secure multiparty computation (SMC)** allows collaborative processing across fog nodes without revealing private inputs, mitigating insider threats. Furthermore, **elliptic curve cryptography (ECC)** and lightweight block ciphers offer strong security with minimal computational overhead, making them well-suited for resource-limited fog devices. By integrating these advanced methods, the security layer evolves beyond generic textbook encryption to reflect current, fog-relevant approaches that directly address vulnerabilities like distributed trust boundaries, insider risks, and constrained resources.

3.1.6 Application or Transport Layer

Initially, fog computing was primarily driven by the application layer [37]. Subsequently, certain applications based on Wireless Sensor Networks (WSN) have adopted fog computing support. Any application experiencing latency issues can now leverage the advantages of the fog environment. This category encompasses utility services seeking enhanced efficiency and cost reduction through fog utilization. Additionally, the fog infrastructure holds potential for systems utilizing augmented reality applications, as it can revolutionize current practices and pave the way for future advancements. By deploying augmented reality in a fog environment, there is the potential for significant and continuous improvements in various augmented reality

applications, particularly in meeting real-time processing demands. The paper provides an overview of fog computing, which a distributed computing paradigm that extends cloud is computing to the edge of the network.

The paper highlights the different security threats and potential application areas of fog computing, providing a brief understanding of the fog's presence in the area. The paper concludes that fog computing has the potential to address many of the challenges facing the Internet of Things (IoT) and other distributed computing environments. The paper emphasizes the need for more research in the areas of security, privacy, and communication to ensure that fog computing is a secure and reliable computing paradigm. The paper proposes a taxonomy of research papers in fog computing, but it is limited to technology and tools used but not focus on the current methods and approaches to provide the security in FC environment, hence it is not clear how comprehensive or representative this taxonomy is of the entire body of research in this area.

3.2 Characteristics of Fog Computing

- *Heterogeneity:* Fog nodes must be deployed following their platforms, which must be extraordinarily dynamic and heterogeneous, to attain the needs of low delay and scalability. The emergence of fog nodes can occur at several network hierarchy levels. A virtualization infrastructure offers processing, networking, and memory capacity among cloud applications, display equipment, and edge devices.
- *Interoperability:* The fog system can cooperate to offer various services and support, providing a broader spectrum of network connectivity.
- *Geographical distribution:* Unlike centralized clouds, cloud computing can be deployed anywhere and has an extensive geographic reach to provide premium services for terminal devices.
- *Large-scale sensor networks:* Cloud computing has been introduced to sensor networks for decentralized processing and storage.
- *Low Latency:* Fog nodes make low latency possible, which provides localization and helps end devices in numerous places.
- *Scalability:* Large-scale sensor networks monitor our immediate environment. The fog's scattered processing and storage resources can support large end devices.
- *Mobility support:* Connecting directly between mobile devices is among the main characteristics of cloud protocols or apps, which support mobility strategies and enhance service performance and quality.
- *Wireless access:* There is minimal capability to facilitate transportation, and with such a wireless device, adjustability is among the determinants that dominate the fog computing access network.
- *Real-time interactions:* Exchanges across cloud servers promptly are supported instead of data entry in a fog.

3.3 Notes About Similar Paradigm

3.3.1 Cloud Computing

Cloud computing aims to consolidate computing and storage in data centers that combine powerful machines with fast connectivity [38]. Within a few years, cloud computing could overtake all other technologies. Since it is a distributed, parallel system, it is possible to dynamically provision and alter the shared resources. The cloud emphasizes centralization. Fog builds on the cloud and connects the cloud to the network edge. There are three main types of services offered by fog computing Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). However, real-time applications are not well suited for cloud computing. Edge computing is available to get around the cloud's constraints. The computing domain includes mobile cloud, mobile edge, and mobile fog.

3.3.2 Edge Computing

A novelty of network edge execution computing is called edge computing. Ad hoc computing and channel resources located among that information on the path at the cloud computing center are referred to as the edge [39]. An Internet of Everything is represented by the uplink data of edge computing, while the downlink data represent cloud services. The endpoints of the cloud are connected to the edge devices. Thus, edge computing provides high-response computing capabilities to end users. IAAS, PAAS, and SAAS cloud model services are not tied to this type of computing.

Along with accessing services and information from the cloud, devices at the network edge also analyze, store, cache, and load balance data transmitted. Therefore, the cloud must be capable of meeting requirements for distinction, extensibility, isolation, and reliability. Edge computing practitioners must be aware of various difficulties, including system reliability. Since processing takes place nearer to the database origin, edge computing has the advantage of enhancing data security. Cloudlets, fog computing, and mobile cloud computing are three edge computing applications.

3.3.3 Mobile Cloud Computing

To enhance user experience (UX) effectiveness or provide greater efficiency for mobile users, mobile cloud computing (MCC) successfully combines the services of cloud computing, mobile computing, and wireless access communication. In mobile network processors, storage and virtualization are performed remotely using portable gadgets [40]. Applications are used for mobile clouds to transfer data from connected cellular gadgets to the cloud for data storage and processing. MCC also offers a range of apps as well for users of mobile and smartphones. Due to a limitation of MCC, where the end user and remote center are geographically separated, mobile apps will grow out of control. The MCC does not apply to many mobile applications because they are necessary for mobility.

3.3.4 Mobile Edge Computing

This recent edge computing mobility periphery computation architecture development combines cellular connectivity with cloud computing capabilities. The European Telecommunications Standard Institute (ETSI) first introduced this idea in 2014, describing it as providing IT and cloud-computing capabilities within the Radio Access Network (RAN) close to mobile subscribers [41]. MEC is designed to let mobile devices offload their computationally expensive activities to servers nearby, thereby reducing latency and battery consumption. The objective of MEC is to move infrastructure as a service for an interface at the program that can succeed with significantly reduced variability, high computing, high bandwidth, minimal stress on the core network, increased quality of experience (QoE), and efficient resource use. There are two types of components in MEC: computer and communication.

3.3.5 Fog Computing

Fog computing, which adds an abstraction layer of resources to integrate the computation resources of participating devices, is the most widely used edge computing approach. Since cloud computing is a hierarchical network and fog is a decentralized distributed architecture, they are fundamentally distinct. They complement one another to make the best use of the resources at hand [42]. Between distant servers and hardware, fog computing serves as a conduit, controls which data should be transmitted across the network, and permits local processing. An intelligent gateway named fog offloads to the cloud for better data retention, processing, and analysis. Here, network resources, such as routers and specialized computer nodes, are used to perform generic application logic. Edge computation is also carried out through fog computing, which blends mobility virtualized and wireless perimeter computers to serve IoT applications.

3.3.6 Cloudlet

A different method of edge computing is called cloudlets, in which small data centers have erected the boundary of nodes to successfully discharge computation, lowering the load at the core network and reducing communication lag [43]. A trusted group of nodes known as a cloudlet makes services accessible to neighboring mobile devices. The resources for the offloading mechanism for mobile devices are provided by cloudlet nodes, which are tiny clouds that are usually only short and geographically distant from smartphones. Cloud service providers that seek to improve latency and energy consumption on mobile devices by having their services available close to such devices are operators for cloudlet computing. Computing with cloudlets is equivalent to MCC and MEC. MACC (Mobile and Cloud Computing) is resource-constrained on mobile devices, although cloudlet computing promotes mobility.

On the other hand, cloudlets do not concentrate on interactions with the cloud and can function as independent clouds. One way that cloudlets and the MEC differ is in this regard. Another distinction is that MEC may use alternate lightweight virtualization methods like containers, whereas cloudlets exclusively use virtualization based on virtual machines.

While Singh (2021) and other recent surveys have broadly categorized fog computing security challenges into the domains of network, data, and privacy, their classifications remain primarily descriptive. In contrast, the taxonomy presented in this work emphasizes fog-specific dimensions that earlier studies have not sufficiently addressed. For example, we identify insider threats at the fog-node level, the impact of mobility on dynamic trust management, and the need for lightweight cryptographic mechanisms to accommodate resource-constrained devices. By highlighting these underexplored issues, the proposed taxonomy advances existing groupings and provides a more focused framework for analyzing the evolving security landscape of fog computing.

3.4 Application of Fog Computing

In some fog-based studies, these users' access has been characterized based on industry and home [45]. This work offered a generalized version based on an exhaustive evaluation of the research material that has been completed in the area of darkness activities in smart buildings concerning confidentiality and security problems [46] and offered inexpensive maintenance for fog-based monitoring. That

technology also has efficient wearable applications and digital controllers. Additionally, devices captured the body's temperature, respiration rate, and treatment to patient readings, sending the data electronically to terminals to provide notifications after a computerized examination.

4 Analysis of Fog Computing Security

By tackling the major technical problems and complexity of cloud computing, fog computing provides a new interaction platform. However, the security and privacy solutions of cloud computing cannot be directly applied to fog computing due to its unique characteristics such as spatial dispersion, heterogeneity, and mobility. These features introduce new attack surfaces and vulnerabilities. Hence, novel and adaptive security mechanisms are essential to address protection and confidentiality challenges in fog computing. While fog computing offers benefits like low latency and scalability, it faces significant hurdles in secure deployment, especially in sensitive applications such as healthcare, industrial IoT, and smart cities [47].

4.1 Attacks on Fog Computing

Fog computing security continues to evolve, but much of the available research focuses only on categorization rather than providing in-depth analysis of individual attacks. This section expands key threats by detailing their **impact, mitigation strategies, and application relevance.

4.1.1 Trust Issues

- **Impact:** Open and distributed fog networks lack centralized control, making trust establishment among heterogeneous nodes difficult. This can lead to data tampering or unauthorized service usage.
- **Mitigation:** Blockchain-based consensus, reputation management systems, and trust-aware authentication protocols are proposed to enhance reliability [48].
- **Application Relevance:** Particularly critical in vehicular fog computing, where trustless nodes could inject false traffic information, endangering safety.

4.1.2 Malware Attacks

- **Impact:** Malware such as ransomware, worms, and Trojans can compromise fog nodes, disrupt services, or exfiltrate sensitive data. Their detection is difficult due to resource constraints of fog devices.
- **Mitigation:** Lightweight anomaly detection, sandboxing, and distributed intrusion detection systems (IDS) tailored for fog environments [49].
- **Application Relevance:** A major concern in smart healthcare, where malware can disrupt patient monitoring systems or alter medical records.

4.1.3 Data Processing Exploits

- **Impact:** Errors or manipulations during fog-level data processing may lead to integrity breaches, privacy leakage, or unreliable decision-making.
- **Mitigation:** Secure multiparty computation, encrypted data processing, and integrity verification mechanisms\ [50].
- **Application Relevance:** Especially relevant for smart grids, where faulty data aggregation at fog nodes may destabilize power distribution.

4.1.4 Man-in-the-Middle (MITM) Attacks

- **Impact:** Attackers intercept communication between fog nodes and users, leading to data theft or manipulation.
- **Mitigation:** End-to-end encryption, secure key exchange, and mutual authentication protocols [51].
- **Application Relevance:** Critical in mobility-driven healthcare systems, where intercepted medical data can compromise patient privacy.

4.1.5 Collusion Attacks

- **Impact:** Multiple malicious nodes may collaborate to amplify attack impact, such as launching coordinated denial-of-service attacks.
- **Mitigation:** Game-theory-based detection, cooperative IDS, and trust-weighted voting mechanisms.
- **Application Relevance:** Severe in IoT-based industrial control systems, where colluding nodes can halt or manipulate production.

4.1.6 Virtual Machine (VM) Attacks

- **Impact:** Adversaries exploit hypervisors to compromise virtual environments, leading to VM escape, inter-VM data leakage, or full system takeover.
- **Mitigation:** Hypervisor hardening, resource isolation, and continuous monitoring for abnormal VM behavior\ [52].

- **Application Relevance:** A pressing threat in industrial IoT deployments, where virtualization is widely used for workload distribution.

4.1.7 Node Attacks

- **Impact:** Physical compromise of fog nodes may allow attackers to extract sensitive data, manipulate hardware, or disable services.
- **Mitigation:** Tamper-resistant hardware, secure boot mechanisms, and physical monitoring of critical nodes.
- **Application Relevance:** Crucial in smart city infrastructure, where edge nodes control traffic lights, surveillance cameras, and energy systems.

4.1.8 Privacy Preservation Threats

- **Impact:** Leakage of sensitive information such as user identity, location, or behavior patterns threatens confidentiality.
- **Mitigation:** Privacy-preserving cryptographic schemes (e.g., ECDSA), homomorphic encryption, and anonymization techniques [54].
- **Application Relevance:** Vital in IoT-enabled households and enterprises, where unauthorized profiling of user activities poses serious risks.

Additionally Fig. 4 illustrates the key security issues in fog computing, including malware, node attacks, and denial-of-service threats. These attacks are particularly severe in fog environments due to inherent resource constraints, heterogeneous devices, and distributed trust boundaries. For example, node attacks exploit the limited computational power of fog nodes, while malware propagation is accelerated by the mobility and proximity of connected devices.

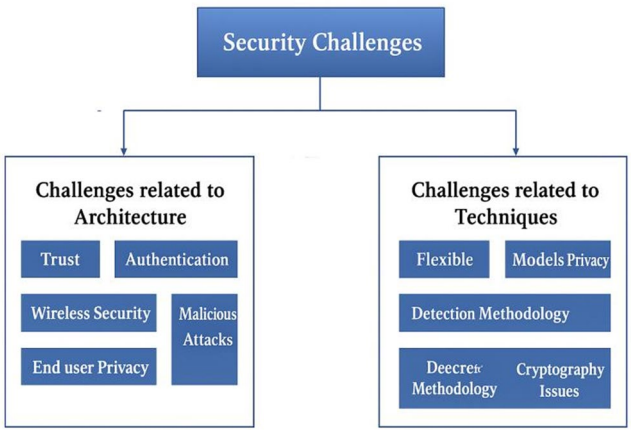

Fig. 4 Issues of fog computing

Similarly, denial-of-service attacks are amplified by the restricted bandwidth and storage capabilities of fog systems, which reduce resilience compared to cloud platforms. By situating these threats within the broader context of fog security, the figure underscores how these vulnerabilities directly compromise system reliability, data confidentiality, and service availability.

4.2 Network Security in Fog Computing

Most cloudlets are networked, and individuals' equipment performs calculations. Thus, it is challenging for the fog computing process to provide security for network services through data because of the large number of users [55]. The infrastructure and information protection of fog is thoroughly covered in this subsection. Information security must be a top priority because of the appropriate network infrastructure in the cloud. Based on this, network security is classified into five divisions Authentication, Access Control, Virtualization, Detection System, and Trust Management, as discussed by recent research papers.

4.2.1 Authentication

People often access several services at once. They should be required to use various authentication methods in various applications. On the other side, the user encounters numerous challenges when trying to keep track of their login information for various facilities. In this way, the biggest problem with the protection of sensor networks is identification [56]. Several critical data breaches for edge computing would weaken authentication that endangers smart objects, the service, and the cloud. Hence, multifactor authentication methods have been suggested to enhance controls in edge computing, but every verification methodology has its advantages and disadvantages. Therefore, the constraints and disadvantages of a few standard digital certificates, including login information registration, PKI-based authorization, and face recognition, are discussed in this paragraph for each branch.

4.2.2 Password-Based Authentication

The password-based authentication scheme is suitable for controlling the hidden information assault. This authentication requires a password from the user for each service. Following that, the administrator maintains all users' names and their passwords on the server, granting access to both physical and virtual devices to a client. As a result, password authentication has many uses and is used in cloud computing. However, fog computing has many disadvantages and restrictions, including a large amount of computation to

process, lack of end device resources, and lack of severe problems due to various attacks, such as offline dictionary attacks, and leakage attacks. Thus, the effectiveness of a key in an encrypted communication protocol in a cloud infrastructure varies on its level of convenience, durability, and security vulnerabilities [57]. One study [58] created an identification scheme involving suitable route discovery among the cloud, fog, and client for secure information distribution. The suggested protocol was evaluated using the Scyther simulator, and parameters proved that strong protection is provided during the execution of the protocol, successfully achieving data flow amid the cloud and fog.

The OTP-based Two Channel Authentication Mechanism (OTPTAM) was proposed in [59] to authenticate the fog nodes. The blockchain database was used to store the data, and communication was achieved using encrypted channels by Elliptical Ciphers to resolve the unprotected password exchange and leak. In addition, the Sybil attack was controlled to prevent the threats of fog nodes, such as stealing data and taking control of the network. The comparative analysis of password-based authentication has been shown in Table 1.

The popularity of password-based authentication CFsec [60] prevents various attacks, and they have limitations to the password. Besides, energy consumption, computation, and delay are considered major challenges.

4.2.3 PKI-Based Authentication

By providing identity and effective management services that enable decryption and signature capabilities across programs in a straightforward and user-friendly manner, critical public infrastructure (PKI) secure authentication establishes and maintains a dependable virtual network. PKI provides communication with authenticity (CIA) and non-repudiation. It is a safety concern while concentrating on verification problems at differing levels of the fog computing system. Also, because the PKI-based procedure can be problematic in a multiuser environment, it is ineffective in the specific situation of cloud computing. The consumer of fog typically has limited resources, meaning they lack the processor and memory power necessary to complete the encrypted procedure. The distribution of authentication tokens can also be challenging because of the massive number of fog devices and end customers.

The maximizing security on real-time communication of different services (MX-SORTS) algorithm was used for network traffic. However, it is not suitable for industrial applications. The multimodal and meaningful transformer networking of one of the leading production networks is incompatible with the public key system (PKI) and secure communications component layer (SSL/TLS) versions of the standard encryption framework [61].

Since Blockchain-based IoT (BIoT) services are implemented in a proprietary and autonomous manner, trusting IoT-based services becomes a crucial issue. To build confidence in BIoT services, the study [62] developed a general architecture design that uses Public Key Infrastructure (PKI). Based on our testing, this has the potential to be a solution to the trust issue and is scalable.

In such shared fog computing environments [64], proposed the Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) key exchange algorithm and Internet of Things (IoT) device based on the publication Message Queuing Information Transportation (MQTT) interface. A certification path was suggested using the Meta-PKI via partition-based technique when considering [63]. By creating partitions based on the validity of certificates, the approach decomposes the data encryption assurance graph.

Physical Unclonable Function (PUF) was developed in [65] to overcome certified authentication and revocation and make the key expansion easier. Additionally, the suggested approach satisfies the essential requirements of the PKI scheme security. Moreover, PUF-based trust relationships incorporate Elliptic Curve Cryptography (ECC) for producing asymmetric key pairs while requiring less power, storage space, and infrastructure setup. The comparative

Table 1 Password-based authentication reviews

Ref. No.	Approach	Strengths	Limitations	Fog-Specific Notes
[58]	Password-Based Key Exchange Protocol	Simple, user-friendly, widely adopted for establishing secure sessions	Vulnerable to dictionary attacks, replay attacks, and weak-password risks	Suitable for small-scale fog deployments but less effective in highly mobile or resource-constrained environments
[59]	Time Password-Based Two-Channel Authentication using Blockchain	Adds temporal factors (time-based one-time passwords) with dual-channel verification; blockchain ensures tamper-resistance	Computationally intensive due to blockchain overhead; requires reliable synchronization	Strong candidate for **vehicular fog networks** and **critical healthcare systems** where auditability and tamper-proofing are vital
[60]	Password-Based Secure Communication Protocol (CFsec)	Enhances traditional password schemes by integrating lightweight cryptographic functions; resistant to eavesdropping and replay attacks	Still relies on user password quality; scalability issues in very large fog networks	Practical for **IoT-fog integration**, providing secure session establishment with low resource overhead

Table 2 PKI-Based authentication approaches in fog computing

Ref. No.	Techniques	Application	Advantages	Challenges/Trade-offs in Fog
[61]	Adaptive Encryption Service (MX-SORTS)	Real-Time Substation Communication	Efficient in handling encryption delays for time-critical communication	Reliability issues under heavy load; requires stable synchronization in fog layers
[62]	PKI-based Trust of Blockchain using IoT Authentication	IoT Applications	Enhances authentication trust by combining PKI with blockchain	Computational complexity and storage overhead may limit deployment on resource-constrained fog nodes
[63]	Certification Graph Building on Meta-PKI (Partition-based)	Blockchain-enabled Applications	Improves processing efficiency of certificate validation	Increased complexity and computation overhead reduce suitability for latency-sensitive fog use cases
[64]	PSK with ECDHE Data-Exchange	IoT Applications	Strengthens security with lightweight algorithms; energy efficient for constrained devices	Higher computation time compared to basic symmetric key exchange
[65]	DRAM-based Physical Unclonable Function (PUF)	Cybersecurity in Fog/Edge Devices	Time-efficient, energy-aware, and resistant to cloning attacks	Reliability variations due to environmental factors (e.g., temperature, aging of DRAM cells)

Table 3 Biometrics-based authentication approaches in fog computing

Ref. No.	Techniques	Application	Advantages	Challenges/Trade-offs in Fog
[66]	Handover Authentication	Communication Applications	High reliability; strong privacy protection; encryption ensures resilience against insider and exposure attacks	Computationally intensive during frequent handovers; may increase latency in mobility-driven fog
[67]	Blockchain-based Biometric Authentication	IoT Applications	Low resource usage and cost-effective; decentralized trust through blockchain	Blockchain integration adds computational overhead; scalability may be affected in dense fog environments
[68]	Multi-Factor Biometric Authentication	IoT Biometric Applications	Strong defense against theft and spoofing attacks; enhanced assurance	High energy consumption and sensor overhead; limited applicability in battery-powered fog devices
[69]	ECC-based Lightweight Remote User Authentication	IoT Communication	Efficient in handling several attack vectors; ensures secure and lightweight authentication	Limited by resource constraints; may struggle with large-scale, real-time fog communications

analysis of PKI-Based Authentication has been shown in Table 2.

4.2.4 Biometric Authentication

Generally biometric traits are commonly used to regulate access to either real or artificial materials. This methodology is used to verify users' biological inputs obtained by biometric scanning or analysis of the user's various body regions. This new technique is already being used in cloud computing, with fingerprint, key stroke-based, face, and touch-based authentication. However, these systems have many limitations and downsides in shared fog computing. For instance, it takes a long time to execute and remains confined when strong security is needed. Therefore, considering biometric authentication is still causing research problems for fog computing.

According to information research, FogHA can withstand known assaults, has a high handover efficiency and avoids duplicate messages with the help of fog networks [66].

The authors of [67] presented an authentication system that secures user authentication by leveraging the benefits of transactions and consensus mechanisms. It seeks to handle user identification in a decentralized setting and protected cloud services issues for technology, such as the Internet of Things. The additional authentication was modified with blockchain using the distributed authentication system. The blockchain was performed efficiently to handle the authentication problem. At last, this suggested system presented the solution to the challenges of fog services.

A novel technique is also proposed to address the security issue caused by fog computing the publication [68]. The strategy was developed that combines various biometric techniques to validate the authenticity of a person and gives a complete model that can provide an essential degree of verification in fog computing. Another study [69] investigated the SAKA-FC protocol and discovered the vulnerability to system attacks, information attacks, and replay attacks. As a result, fog-centric cloud communication, an enhanced, lightweight, and secure authentication technique, were provided. The comparative analysis of Biometrics-Based Authentication has been shown in Table 3.

4.3 Access Control in Fog Computing

Access control in fog computing is essential to take the concern to enhance security by allocating authorized users to access the resources. This access control can restrict unauthorized use by denying the access guarantee by finding the valid user, detecting the attacks, and further preventing unauthorized users. Generally, the access is provided to the user as tenants in fog computing. It is not allowed for anyone to access the service. Users who want to store the data and access the services should accept the policies. It is necessary to understand how to build the policies to fulfill design objectives and resource restrictions for preserving user privacy and ensuring the system. These access control restrictions apply for cloud, fog, and Virtual Machine sides. One of the primary challenges of access control is resource limiting in fog computing. Due to the computation, resources available on the network's end are restricted.

4.3.1 Access Control Requirements

Access control has developed policies to operate fog computing, which can be attributed to the computational overhead. A number of users cannot access the limited resources available in IoT. In fog computing, access control systems must make access choices at a good time. However, some of the present issues of the need for access control as follow,

4.3.1.1 Latency It can be caused by the response time, execution time, and policy decision speed. The provision of minimum-delay services and applications to end users is critical in fog computing.

4.3.1.2 Efficiency Access control efficiency remains difficult for every access control system capable of implementing any policy. It could cause the decision-making process to be late and not accept another network service.

4.3.1.3 Generality The applications and services are achieved in fog computing by utilizing various hardware and software based on technologies. Because of the heterogeneity of fog devices and specialization, top-layer services and applications must be supplied. To interact with current APIs and protocols, generic APIs are required.

4.3.1.4 Aggregation Data is gathered via geo-distributed devices. To reduce latency, fog devices closer to users must aggregate the data. Because user device data may be worthless, aggregation must be done wisely and efficiently. It is challenging to deal with data authority changes before and after aggregation.

4.3.1.5 Privacy Protection Preserving data privacy is a fundamental necessity in fog access control because of the decentralized design of fog computing. This is because data sharing on the client side and at the network's edge is monitored to avoid unauthorized user access.

4.3.1.6 Policy Management This is an essential component of fog computing. Thus, the access control model in fog computing must handle releasing, invoking, deleting, and setting policies.

4.3.2 Models of Access Control

4.3.2.1 Access Control Based on Attributes (ABAC) The organization's data-authorized user sets the rules of policies in AC. These rules might define the users' behavior [76]. ABAC analyzes the attributes of users or resources against the rules. Based on the attributes, access permission is allowed to users and resources access.

4.3.2.2 Access Policy Access Control Model (APAC) APAC, called data-based access control, determines a subject's authorization to conduct operations by analyzing attributes in certain situations and environments. It allows permitting users to access specific resources [77]. The authorized user develops the policies using the data with security objectives.

4.3.2.3 Model of Role-Based Access Control (RBAC) The role-based access control depends upon the user's role, not considering the users.

Sometimes, some users may hold many roles inside the company. This AC policy analyzes the defined RBAC by the owner and permits the role-based users to view, read, update, and/or write in this model. The user's role is matched to the access policy set by the owner, then the user seeking data is provided access [78].

4.3.2.4 Usage Control-Based AC This access control starts the actions after the user operates, such as writing, reading, etc., and includes some characters to manage user control in fog computing. To do so, an action is evaluated using access decisions and also monitored through control con-

tinuity. It introduces the attributes mutability for the usage of resources. Besides, it provides the authority to allocate the resources to predict the objects and subjects based on defined authorization, condition, and obligation policy.

4.3.2.5 Reference Monitoring Access Control (RMAC) RMAC provides access permission to the authorized user to access the resources and makes the operation based on reference validation mechanisms with decision-making requests. The reference validation system must have various characteristics, including evaluability, invisibility, non-bypass ability, and tamper-proof.

However, in typical systems, the Reference Monitoring Access Control is unsuitable for dynamic distributed systems. High latency and processing costs are applicable when accessing the entire request due to its central-based design. In [80], proxy re-encryption (PRE) was achieved to overcome these issues. The cryptography primitives convert the cipher text through proxy. Meanwhile, some characteristics of secure fog commuting include non-interactivity, unidirectionality, proxy invisibility, non-transferability, collusion safety, key optimality, and chosen-ciphertext safeness. The comparative analysis of Access Control security has been shown in Table 4.

4.3.3 Model of Discretionary Access Control (DAC)

Identifying the users who seek access is done to control access in this AC model. The user has the authority to develop the access policy and decide to access permission for others [81]. The inheritance applications only perform in DAC cause large users and applications able to access fog computing. Despite this, the UNIX operating system environment was incorporated with more flexibility and low security.

4.3.4 Identity-Based AC (IBAC)

The active entity, passive entity, and access rights are mainly three interactions in IBAC. It identifies the users and resources and performs specific operations like read, delete, and write. IBAC allows users to access the resources with specific operations based on policies [82].

4.3.5 Access Control Based on Tasks (TBAC)

This paradigm controls access by matching security labels to security clearances. A task is regarded as a sub-role for a subject in this approach. When a subject's task fulfills the roles incorporated in action, the action is given access to a user [83]. Each object, such as a resource, is assigned a label indicating the critical resources. The labels are made up of two parts of components classification and category components that decide the accessible objects. A classification and category are assigned to the subject, who is a user. When an object attempts to access a resource through MAC, it examines the user's classifications and categories and compares them to resource labels. If the user's categorization and category match the labels of a resource, access is granted.

4.4 Virtualization

Many studies have been conducted on fog-IoT networks as task offloading. Even though one critical offloading problem has received little attention, namely the influence of various virtualization options on task reaction (TR) time, this work bridges this gap by characterizing the TR time for each with three virtualization modes. The fog's virtual machines (VM) are tailored uniquely in each mode,

Table 4 Access control (ac) security of fog computing

Ref. No.	Model	Techniques	Advantages	Challenges/Trade-offs in Fog
[76]	ABAC (Attribute-Based Access Control)	Policy Retrieval Method	Policy evaluation is 3–5× more efficient; improved scalability	Requires reduction of policy scale; computational cost increases in large, dynamic fog networks
[77]	APAC (Attribute and Policy-based Access Control)	IoMT with IP-enabled WSN + Blockchain	Secure, feasible, and rational; integrates IoT and blockchain for enhanced trust	Vulnerable to resource depletion attacks; group key management and publishing lack flexibility
[78]	RBAC (Role-Based Access Control)	Lightweight Graph-Based Model (LiCo)	Lightweight and simple to implement	Limited adaptability in dynamic fog settings; lacks comprehensive evaluation of security and performance
[79]	ABADC (Attribute-Based Access and Data Control)	CP-ABE (Ciphertext-Policy Attribute-Based Encryption)	Provides access control, verification, and confidentiality; two-step encryption improves efficiency	Increased encryption complexity; higher latency in real-time fog applications
[80]	RMAC (Role and Multi-Attribute Control)	Multi-Stage Classification (MSC) in WSNs	High energy efficiency; supports priority-based immediate transmissions for critical conditions	Lower energy consumption compared to RTBDG, but scalability and policy adaptation remain challenges

exploiting VM elasticity. The perfect virtualization mode is tailored to fit the computational load of the incoming workload exactly. This promotes that each job receives the same service time regardless of the VM assigned. EnTruVe's VM allocation algorithm provides a more extensive selection pool of v-fogs that fulfill the VM's requirements (e.g., trust, latency), ensuring a better possibility of VM allocation success. In semi-perfect virtualization mode, a less rigorous and thus more practical option, the VM configured to match the EnTruVe roughly is an Energy and Trust-aware VM Allocation in Vehicle Fog Computing solution that tries to reduce VM processing associated energy usage as much as feasible [86].

Two semi-Markov decision process (SMDP)-based coordinated VM allocation methods are suggested in [87] to balance the tradeoff between the remote cloud's high cost of providing services and the local fog's limited computing capacity. The Task scheduling algorithm was presented in [88] for energy-balancing. To reduce energy consumption, the schedule requests in real-time, and the dynamic threshold strategy is used, ensuring terminal device energy balancing with the absence of delay.

Through studies, we investigated the impact of VM performing the GPGPU (General-Purpose computing on Graphics Processing Units) activity (GPGPU-intensive VM) on other VMs as shown in Table 5. Then, we suggest alleviating the performance degradation of other VMs by dynamically allocating the VM's resource consumption time and preventing the GPGPU-intensive VM from being prioritized. This activity was analyzed and evaluated using the evaluation to know the performance of the Virtual Machine. At last, allocating the dynamic resource usage time and preventing the priority preemption in GPGPU were achieved to mitigate the performance degradation of other VMs [89].

4.5 Analysis of Detection System

The rapid growth of technologies of the net produces many connected devices. Fog computing has increased attacks, which necessitates the employment of efficient and practical countermeasures to infrastructures of networks based on the damage from cyber-attacks. Intrusion detection systems (IDSs) are crucial to fog network security since they increase service quality. They can also be used on the network to avoid malicious attacks, such as port scanning and denial-of-service (DoS) attacks. Then, it opens up new directions for investigating the potential benefits of centralized and client-side fog computing for intrusion detection.

Its implementation requires determining the IDS system's suitability for a big data environment and completing detection for four different attacks, including DoS (interfering with or denying services to clients), probing (monitoring and other detection activities), R2L (illegally accessing systems or resources for remote systems), and U2R (performing unauthorized access of regular users as well as privileges of administrators in cyber). Based on this, various conventional approaches are available. However, they cannot offer adequate protection because all they do is detect intrusions. Therefore, it is essential to understand the attack category to put the proper defenses against each threat.

Additionally, it could be helpful to identify the user for decision-making, which may also aid the network administrator in making decisions. It may decide to take action to address the vulnerability that was exploited in the attack. Some recent publications analyzing the detection system's security issue are subsequently presented.

The author examined the physical layer security (PLS) [90], which uses the characteristics of the connection between the last user and a fog node to identify impersonation attacks in a fog computing network. Establishing precise channel constraints between the end user and fog node is also tricky. The Q-learning algorithm was developed to achieve the best test threshold value for the impersonation attack. This system shows how impersonation detection may adapt to shifting conditions. The solution's efficiency confirms and guarantees that the impersonation attack in fog computing networks will be precisely recognized. Generally, the attackers transmit malicious data packets to these targets to endanger them. It is challenging to discover these invasions to provide users with a secure and reliable service. Therefore, a robust Intrusion Detection System (IDS) is necessary for the fog to operate securely without losing effectiveness. The method Auto-IF for intrusion detection corresponding to a deep learning methodology employing

Table 5 Security on virtualization in fog computing

Ref. No.	Technology	Application	Advantages/Challenges
[85]	Queuing theory under different virtualization modes in task response time	Any Fog Application	In task response time, queuing theory under various virtualization modes
[86]	EnTruVe	Vehicle Fog Computing	Energy consumption, trust, and latency
[87]	Semi-Markov decision process (SMDP)	Fog Application	Efficient Virtual Machine allocation and attacks are needed to be concentrated
[88]	Energy balancing algorithm -Container-based VM	Wireless Sensor Network application	Efficient task scheduling, low latency, High Energy Consumption
[89]	Mitigation Techniques	Fog Computing	Minimum time and security are needed to be implemented

Table 6 Review of detection system

Ref. No.	Method	Application	Advantages	Disadvantages
[90]	Q-learning algorithm	IoT application	Prevent Impersonation attacks in physical layer security	False alarm rat will be improved
[91]	Auto Encoder Isolation Forest	Health Application	Intrusion Detection	Accuracy and time will be implemented
[92]	SDN controlled Framework	Wireless Network Application	Efficient, timely anomaly detection	More attacks will be considered

Table 7 Review of trust management

Ref. No.	Methods	Application	Advantages	Disadvantages
[93]	TACRM	Mobile Communication	High security is provided between Fog and IoT	Resource allocation is needed to be implemented
[94]	TMSRS	Wireless Sensor Network	Perfect decision-making and efficient attacks prevention	Latency
[95]	Trust based Task mapping	Vehicular	Efficient resource allocation & reduce the task drop with a low period	Vulnerable
[96]	Decentralized Blockchain-Based Trust Management Protocol	Fog Applications	High-speed and efficient resilient attacks	It needed to be implemented in malicious node detection

Autoencoder (AE) and Isolation Forest (IF) was suggested. To distinguish between attack and routine traffic in the present time, our system only considers binary categorization of incoming traffic on a fog device. The Autoencoder was instructed to learn the standard data. Attack data are not correctly encoded when encountered, resulting in more reconstruction loss [91].

The author has introduced an Intrusion Detection and Prevention System (IDPS) specifically designed for Internet of Things (IoT) networks powered by fog-assisted Software Defined Networking (SDN) [92]. This proposed IDPS is designed to swiftly identify various attack models in near real-time, facilitating efficient threat neutralization through SDN control. This effectiveness is achieved by deploying a fog computational setup closely integrated with an IoT network. In this context, the SDN controller plays a crucial role in implementing the necessary flow controls to prevent network edge switches from forwarding attack traffic. By leveraging the capabilities of fog computing and SDN, this IDPS aims to enhance the security of IoT networks by detecting and preventing intrusions in a timely and effective manner. The comparative analysis of Detection System has been shown in Table 6.

4.6 Analysis of Trust Management in Fog Computing

By extending traditional cloud computing to the network edge, fog computing is a decentralized computing infrastructure that brings data, computing, communication resources, and storage closer to end users. Despite this, fog servers should be trusted for delegation because they are positioned near end edges and attain sensitive data. The fog servers have grown accustomed to one another after cooperating. The ability to choose a reputable fog in a field will aid in offering the needed fog services in a high-quality manner. The TMS evaluates direct and indirect trust based on previous reputation and recommendations, as well as the quality of service (QoS), quality of security (QoS), and social ties.

Furthermore, because fog trust is dynamic rather than static, fog A may trust fog B at a specific timestamp (e.g., time1) but distrust fog B at time2 for two reasons. First, the topology of fog networks is constantly changing as nodes are added to or removed from the fog domain. Second, malicious assaults within the domain could cause fogs to behave differently (e.g., DoS). Traditional cryptographic techniques cannot be used to defend against internal threats like those posed by rogue fog that has been verified and integrated into the system. Therefore, regular trust evaluations are crucial. Table 7 presents several works to improve trust management in fog computing.

Fog computing confronts serious privacy issues due to its properties, like heterogeneity, mobility, and vast-scale geolocation. As a result, we suggest a security model that relies on IoT and fog collaboration. This model incorporates an effective access control method linked to a monitoring scheme to enable secure collaboration between various resources and operational components. To enhance the expected system performance, a thorough scheduling method and resource allocation mechanism model are suggested [93].

A Gaussian distribution-based comprehensive trust management system (GDTMS) for F-IWSN was proposed to increase transmission security. Additionally, grey decision-making was added to the trust decision to achieve the trade-off between transmission efficiency and energy

consumption. The suggested trade-off can successfully choose a trust management-based secure routing strategy as the reliable and secure relay node. The above strategies can also be used to defend against bad mouth attacks [94].

Task mapping involves the need for a trust-based solution, as each task comes with unique characteristics such as expected completion time and specific trust requirements that must be satisfied. In the context of 5G networks, a framework has been proposed to calculate the trust value of off-street vehicle fog computing capabilities, organizing clusters of vehicles based on these trust values. Tasks can then be shared among vehicles in the same cluster that meet the trust requirements for those tasks [95]. For widely distributed Internet of Things (IoT) devices, a blockchain-based trust management protocol is presented by Across Trust management, offering mobility support. This protocol entails mobile smart objects distributing service provider trust data to the blockchain. The architecture ensures that every object comprehensively understands every service provider, expediting the trust evaluation process. Additionally, the protocol demonstrates resilience against common detrimental assaults, including vote-rigging, slander, and coordinated attacks [96].

4.7 Data Processing

Big data processing is currently a concern for cloud and mobile cloud big data architecture. A federation of clouds and fog can take care of the gathering, aggregating, and preparing of big data by reducing the costs associated with data transportation and storage and balancing computation resources on data processing. Fog gives elastic resources to large-scale data processing without the noticeable delay associated with clouds. The data processing issue in IoT is one for which fog computing is emerging as an appealing solution. This is because it relies on network edge devices that are more powerful than end devices and closer to them than more powerful cloud resources, lowering applications' latency. While it sounds simple and places data processing as near to the user as possible, this paradigm shift significantly impacts communication methods, lowers latency, and raises service quality.

In the ecosystem, end-user devices frequently transmit data processed by the cloud system to the fog nodes, while also receiving information from the cloud. The quantity and characteristics of data transmitted from end users to cloud systems and from fog nodes to the cloud undergo changes through multiple stages. Fog servers manage caching, computation off-loading, heterogeneity management, and the transmission of data from mobile devices and sensors to the cloud system. Following their journey through the cloud, data sent from end users and data delivered from fog nodes to the cloud undergo alterations in size and nature due to various processes. An additional challenge arises from the fact that numerous providers possess these fog nodes, making it challenging to instill trust in them due to the numerous security and privacy flaws that may result from data processing. The intricacies of data distribution in fog computing are extensively explored in the following subsections.

4.7.1 Data Distribution in Fog Computing

Fog computing can solve problems with data distribution by conducting heterogeneity, mobility support extension, and data dispersion. Data storage strategies span many study areas, including data distribution, dissemination, and replication. By evenly distributing data to entire nodes in large-scale networks with plenty of cooperating devices, data distribution algorithms can free up storage space. In fog computing, data should be disseminated to fog nodes. Large organizations like Amazon and Google enhance their solutions to satisfy their storage needs in complex infrastructures and incredibly demanding settings. Table 8 presents some research on data distribution in fog computing.

A decentralized fog-based storage system created specifically for IoT data is described by [97]. To use object storage, Software Defined Storage (SDS) and the optimal data distribution among scattered mini-Clouds are suggested.

Table 8 Review of data distribution security for fog computing

Ref. No.	Methods	Application	Advantages	Disadvantages
[97]	Optimal Software Model Defined Storage (SDS) for data distribution	Fog Application	Efficient data sharing, storage	Redundant data will be reduced
[98]	Bio-Inspired m model data distribution	VANET	Efficient Data Availability, Minimum Data Replication	Data Ownership issue
[99]	Fair data storage distribution	IoT Application in Industries	High availability with minimum delay	Illegal Data Access will be concentrated
[100]	Blockchain, Hybrid Consensus Mechanism (Proof-of-Work and Proof-of-Authority)	Fog Computing, Key Management	Ensures confidentiality and integrity of data transmission, Trust-based access control mechanism prevents unauthorized access, Balances security and efficiency of the system	Reliance on blockchain technology may be unfamiliar to some users

However, it assumes that SDS platform-capable devices are present and easily accessible at the network's edge.

Danilo et al. presented a distributed methodology to tackle the problem of data availability and distribution problem in this context, inspired by evolutionary computation and epidemic models [98]. According to simulation results, the technique produces relevant results in sustaining data availability in fog and mist computing environments, even under challenging scenarios.

The study by Marino et al. discusses a unique data distribution and replication storage solution for wireless sensor networks, which is the first to incorporate sensor node heterogeneity to select the optimum storage replication based on node capabilities. The solution was carefully designed to function with even the most basic microcontrollers in many of today's smart gadgets. Data contrasting Mist/Edge with traditional Amazon S3 storage is another input showing plenty to learn about Mist/Edge storage and the industry at large [99].

In [100], the authors have introduced a novel blockchain-based key management system, known as BSKM-FC, with the primary objective of securing data transmission in fog computing environments. This system aims to ensure the confidentiality and integrity of data by encrypting it with robust keys. Unlike traditional centralized key management approaches, BSKM-FC utilizes a decentralized blockchain network to manage the keys, eliminating the need for a single central authority. This decentralization enhances security by mitigating the risk of a single point of failure. BSKM-FC is specifically designed to be lightweight and scalable, making it well-suited for fog computing environments with limited resources. To strike a balance between security and efficiency, the system employs a hybrid consensus mechanism combining proof-of-work and proof-of-authority. The authors further propose a trust-based access control mechanism to ensure that only authorized users can access the data. A reputation score is used to evaluate the trustworthiness of users and devices, enhancing security and preventing unauthorized data access. The potential benefits of the BSKM-FC system include improved security and privacy in data transmission within fog computing environments. Additionally, its scalability allows adaptation to diverse use cases and environments.

4.7.2 Data Processing for Fog Computing

A flaw in attribute-based signature and ciphertext-policy attribute-based encryption (CP-ABE) forms the basis of data access control systems. As a result, bad users may work together to decrypt ciphertext that they should not be able to decrypt. We mainly show how the collusion attack could take advantage of the underlying CP-ABE. Table 9 presents several the review of data processing security analysis in fog computing.

The architectural paradigm to generate on-demand edge-cloud processing structures that can be used indefinitely to continuously manage massive health data while also carrying out services for meeting NFRs is presented by Syh-yuan tanetal. To establish edge-fog-cloud processing structures, this approach recursively connects constructive and modular components implemented as micro services and Nano services [101].

Continuity methods, which also implicitly enforce the fulfillment of NFRs for data entering and exiting each block of an edge-fog-cloud structure, establish data flows via the blocks of edge-fog-cloud structures. To demonstrate the model's applicability, a prototype was created and tested in a case study based on processing health data for supporting crucial decision-making processes in remote patient monitoring [102].

In [103], a novel anonymous authentication scheme called ANAA-Fog is proposed for 5 G-enabled vehicular fog computing. The primary aim of ANAA-Fog is to provide secure and anonymous authentication for vehicles participating in vehicular fog computing networks. The authors emphasize the importance of anonymous authentication in such networks to safeguard vehicle and user privacy while thwarting potential attacks like impersonation, replay

Table 9 Review of data processing security analysis

Ref. No.	Methods	Application	Advantages	Disadvantages
[101]	Data Access Control With Ciphertext	Cyber Security	Collusion attacks are determined efficiently	Computation
[102]	Micro/Nano service Composition	Health Application	Efficient anomaly detection with accurate decision making	Cost
[103]	ANAA-Fog, a novel anonymous authentication scheme for 5 G-enabled vehicular fog computing	Enhancing security and privacy in vehicular fog computing networks	Provides secure and anonymous authentication, preserves the privacy of vehicles, efficient and scalable	The effectiveness of the scheme depends on the security of the private keys of the vehicles
[104]	An intelligent fog computing surveillance system for crime and vulnerability identification and tracing	Surveillance and security in public spaces, crime prevention, and incident response	Real-time monitoring, intelligent data analysis, improved security and safety,	Dependence on high-quality data and sensors, privacy concerns

attacks, and eavesdropping. ANAA-Fog achieves these security benefits while ensuring efficiency and scalability. ANAA-Fog is structured around three stages: registration, authentication, and revocation. In the registration stage, each vehicle generates its unique public and private keys, sending the public key to the fog node. During authentication, the vehicle sends a request message to the fog node, which generates a random challenge and forwards it to the vehicle. The vehicle signs the challenge using its private key and sends it back to the fog node for verification. Upon successful authentication, the fog node responds to the vehicle, confirming its authenticity. In case of any malicious activity, the fog node has the capability to revoke a vehicle's access during the revocation stage. ANAA-Fog exhibits superior performance in terms of communication overhead, computation overhead, and security level.

In [104], the authors have presented an intelligent fog computing surveillance system designed for crime and vulnerability identification and tracing. Utilizing a network of cameras and sensors in public spaces, the system captures real-time data, which is then subjected to analysis using machine learning algorithms to detect potential threats and vulnerabilities. The system also enables tracking of individuals and vehicles, facilitating the identification and tracing of suspects. The paper highlights several potential benefits, including enhanced security and safety in public areas and improved incident response. However, the effectiveness of the system relies heavily on high-quality data and sensors and may raise concerns regarding privacy.

4.8 Privacy Preserving Security

Fog computing is one of the most prevalent examples of edge systems and a part of the broader Internet of Things concept (IoT). It is best defined as the movement of computing, ideally closer to devices near the end user. Due to the inherent decentralization of fog computing, the security and privacy techniques currently used in cloud computing infrastructures are ineffective. The leakage of personal information like date, location, and usage is getting more attention when end users use services like IoT, wireless networks, and cloud computing, Fog nodes, which are located closer to end users and have access to more sensitive data than remote clouds that are a part of the core network, provide extra challenges for ensuring such privacy. Despite this active research field, there are currently no privacy-preserving frameworks for public cloud computing. Pseudo-anonymization methods employed in current systems can be deanonymized by combining data from many sources. While fog computing can considerably boost terminal device capacity and viability, it poses many more risks. For instance, there could be dishonest brokers. Even worse, a reliable broker could fall victim to threats (such as hacking, bugging, and corruption) from malicious rivals and divulge customer personal data. Due to these security vulnerabilities, the broker is now the weak link in the fog-based PS system. The protection of user privacy is becoming more and more critical. Differential privacy technology has a significant potential to secure data privacy by preventing adversaries from studying data as shown in Table 10. To prevent the statistical opponent analysis from revealing the real data, it artificially noises the data before output.

With this capability, the PS system based on fog can precisely prevent the collusion assault. But in the PS system, the brokers must also match an equivalent or similar interest between the publisher and subscriber. Finding a balance between user privacy and the necessary personality-matching data has become critical and necessary while simultaneously safeguarding the PS system against collusion attacks. The subject of user and location privacy covered in the literature is discussed in the next subsections.

4.8.1 User Privacy

Another privacy concern is how a fog client makes use of fog services. In the event of a smart grid, for example, the smart meter reading will reveal much information about a household, such as when no one is home and when the TV is turned on, which violates the user's privacy. Even though privacy-preserving technologies for smart meters have been developed, they cannot be employed in fog computing since there is no corresponding hardware, such as a battery, or a responsible third party (such as a smart meter in a smart grid). The fog node can quickly gather user usage statistics. One simplistic method is for the fog client to create fictitious jobs and distribute them across numerous fog nodes, hiding its real work amid the fictitious tasks. However, this tactic will cost the customer of the fog more money and waste

Table 10 Analysis of user privacy security in fog computing

Ref. No.	Methods	Application	Advantages	Disadvantages
[105]	Sampling perturbation encryption method	IoT Application	Efficient minimize redundant data and privacy-preserving for users	Time Consumption
[106]	High-order Bi-Lanczos approach	Industrial Application	Efficient, secure storage consumption	High energy cost consumption
[107]	Integer linear programming (ILP) model	IoT Application	High Secure data transmission with low delay	Energy consumption

more time and resources. A different choice would be to intelligently split the application to ensure that the offloaded resource usages do not reveal personal information.

The suggested sample perturbation encryption method safeguards data privacy from prying eyes and active attackers without sacrificing data correlation. It also makes it easier to decode and decompress encrypted sampling data simultaneously. Additionally, the established data processing method at fog nodes dramatically lowers the number of redundant data transmissions, and the formulation of an optimization model for the measurement matrix ensures the high accuracy of data reconstruction at the end user [105].

The High-order Bi-Lanczos (HOBI-Lanczos) technique has proven exceptionally effective in analyzing heterogeneous data in industrial applications [106]. This study suggests a ground-breaking HOBILanczos method for industrial data applications that protects user privacy and uses cloud-fog computing tensor trains. Specifically, a privacy-protecting industrial data analysis method based on tensor trains and cloud-fog computing is initially proposed. Fogs and clouds may safely analyze industrial data for large-scale tensors delivered in tensor train format with the aid of the suggested methodology. This approach also provides a HOBILanczos mechanism for privacy protection.

An integer linear programming (ILP) model and dynamic programming technique were developed to optimize the amount of successfully served IoT data jobs with sufficient security requirements while minimizing the end-to-end transmission delay. An efficient and privacy-preserving carpooling system that offers conditional privacy, one-to-many matching, destination matching, and data audibility was also proposed via blockchain-assisted vehicular fog computing. Data are relevant to carpooling are stored on a private blockchain [107]

4.8.2 Location Privacy

Location privacy in fog computing primarily refers to the privacy of the fog locations of the client. The fog node that receives the tasks can deduce if the fog client is close by or further away from other nodes because a fog client often offloads its work to the closest fog node. Furthermore, if the fog nodes cooperate, a fog client that uses multiple fog services in different locations may reveal its journey trajectory to the fog nodes. A person's or a vital object's location privacy is jeopardized as long as such a fog client is linked to them. If the fog client always selects the nearest fog server, the fog node may be particular that the fog client using its computational resources is closed. Location privacy can only be preserved through identity obfuscation, which stops the fog node from recognizing the fog client even while it is aware of its proximity. There are several techniques to hide one's identity; for example, the authors generate fake identification for every user with the assistance of a responsible third party as shown in Table 11.

A fog node is not needed to select the node nearest to it. Instead, it makes its own decision among the fog nodes it may access depending on criteria like load balance, reputation, latency, etc. In this scenario, the fog node can only roughly determine where the fog client is. However, once the fog client uses several fog nodes in a particular area to process data, its position can be constrained to a small area because it must be placed where the various fog nodes' coverage intersects. The method used in this instance can be used to ensure location privacy [108].

Fog computing will aid in the unrestricted expansion of location services, and because of this, more robust and more secure methods for location privacy are required. Location obfuscation is one method we utilize to change the user's location information. It is possible to do this either irrevocably or reversibly. To resolve the tension between privacy-preserving security and query quality brought on by the precision of location information, a clustering technique that tries to reduce outliers and is based on the k-anonymity location privacy-preserving model is proposed. The construction of an anonymous group in the anonymous model is realized using this technique. The distribution of users in the anonymous group is fair. Instead of using the user's location, it is suggested to use the center of the anonymous group [109].

In [110] authors have developed a novel energy-efficient location privacy-preserving (ELPP) strategy for vehicle networks by utilizing intimate social fogs (SIF). ELPP is based on three state-of-the-art techniques. First, ELPP sends

Table 11 Analysis of location privacy for fog computing

Ref. No.	Methods	Application	Advantages	Disadvantages
[108]	Location Privacy Using Data Obfuscation	GPS	High privacy and feasibility Minimum latency	Energy consumption
[109]	K-anonymity Location Privacy Algorithm	Network Application	Secure location privacy with high QoS	Query service will be implemented
[110]	Energy-efficient location privacy-preserving (ELPP) scheme	VANET application	Energy-efficient, fast and secure.	vulnerability
[111]	lightweight Utility-based Delegated Byzantine Fault Tolerance protocol	5 G communication	Secure, private, and fast	The focus will apply to mobility and traffic density

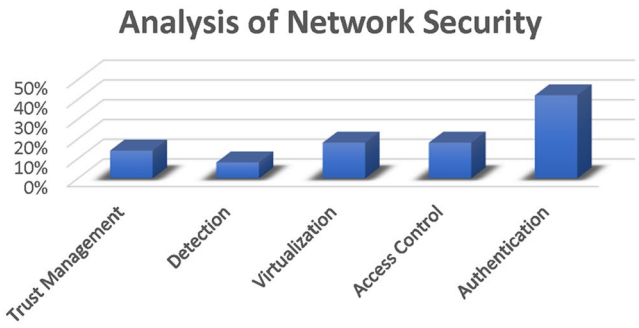

Fig. 5 Network security analysis based on recent research

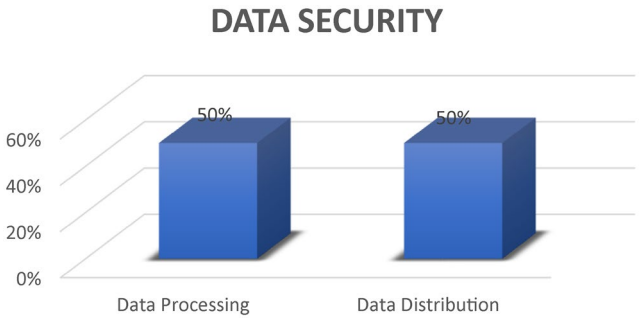

Fig. 6 Data security analysis based on recent research

a sizable number of LBS requests to their SIF for processing. The essential insight is that greater computer efficiency for location privacy preservation can compensate for some communication delays. Second, adding a journey plan-based LBS content pre-caching mechanism enables quick and adaptable retrieval and distribution of the LBS contents. Thirdly, to guarantee confidentiality, ELPP randomly encrypts the data using access control encryption (ACE) [111].

In [112], the authors have presented a novel financial incentive scheme for cooperative location privacy preservation in 5 G-enabled vehicle fog computing. This strategy uses blockchain-enabled consortium fog layers and smart contracts to guarantee dependable and secure cooperative pseudonym-altering operations (PCPs). It also enhances intelligent contracts to reduce transportation costs while retaining a higher level of location privacy. A strong and portable Utility-based Delegated Byzantine Fault Tolerance (U-DBFT) consensus mechanism is proposed to provide speedy and trustworthy block mining and validation.

5 Results and Discussion

The security challenges of fog computing can be categorized as network, data processing, privacy, password protection and identification, attacks, information distribution, user and location, trust management, and virtualization. The

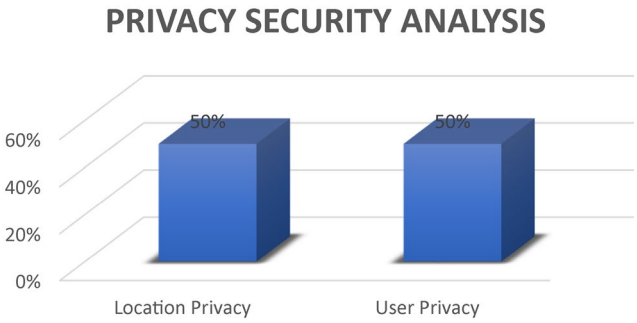

Fig. 7 Privacy security analysis based on recent research

existing approaches reported in the literature, extracted from IEEE, Springer, etc., were analyzed to find the challenges. Accordingly, Figs. 5,6 and 7 display the existing research on fog computing based on the percentage of each challenge mentioned above. We found that privacy makes up 50% of the research, followed by identification and password protection making up 41 and 18%, then dependability or assaults as cyber security with 9%. Furthermore, researchers saw 43% of data distribution in recently published publications mentioning the availability of data, secure sharing technology, or security applications, where several obstacles were caused by weather. Here, we understood that a communication link in 57% of data processing is portrayed in documents as a difficulty.

Recent deployments and experimental studies (2021–2024) indicate that while proposed fog security models demonstrate strong theoretical robustness, their performance in real-world environments is less uniform. For instance, PKI- and blockchain-based schemes improve authentication and trust, but they often incur significant energy costs on resource-constrained fog nodes, limiting scalability in dense IoT deployments. Similarly, biometric and multi-factor access control approaches enhance resilience against impersonation and theft attacks, yet user adoption barriers such as privacy concerns, usability, and sensor reliability hinder widespread deployment. Case studies in smart healthcare and industrial IoT show that lightweight cryptographic protocols and machine-learning-based anomaly detection can be successfully implemented, but latency and interoperability remain practical challenges when integrating heterogeneous fog nodes. These findings suggest that the long-term viability of fog security models depends not only on their cryptographic strength but also on their operational adaptability, cost-efficiency, and user acceptance, highlighting a gap between theoretical security guarantees and deployment-ready solutions.

5.1 Discussion of Network Security

Identifying the challenges and resolving these issues is essential to strengthening network security. By increasing the development of fog computing, the number of end users also increases daily. In this manner, the network is classified into five major topics: Authentication, Access Control, Detection systems, Trust Management, and Virtualization. Initially, the critical role system of the Authentication approach was analyzed through recent methodology, merits, demerits, and application under the subdivision topic of Biometric Authentication, PKI, and Password-based Authentication.

An efficient and privacy-preserving carpooling system offers data audibility and specializes in conditionally anonymous user authentication. As threats and vulnerabilities have increased, an authentication procedure and various authentication approaches have been developed using a novel key exchange algorithm, lightweight algorithm using blockchain, lightweight encryption algorithm, and certification graph protocol. Corresponding to that, Low Computation, Reliability, Energy Consumption, Lightweight, and High Speed are authentication challenges under many applications, such as Cyber, Communication, Healthcare, etc., as shown in Fig. 8.

Secondly, the remaining subdivision topics, such as Access control, Virtualization, Trust Management, and Detection systems, were analyzed to determine the issues in network security of cloud service research. Figure 9 presents the network security challenges. According to that, various methods or technologies are provided to solve the network security issues like latency, cost, energy consumption, lack of detection of attacks, and inaccurate decision-making.

The Scalability, Resource attacks, Energy Consumption, Latency, and computation will be concentrated on the implementation of Network Security required to solve the network security issues.

5.2 Solution for Network Challenges

In this research, authentication based on network security has various approaches to handle encryption efficiency using blockchain. These include key-based protocols and Elliptic Curve Diffie–Hellman Ephemeral (ECDHE) key exchange algorithm to achieve low latency. Sybil attacks, Secret Leakage attacks, Replay Attacks, Insider attacks, Theft attacks, etc., are detected to enhance the authentication approaches. In addition, the lightweight algorithm also considers authentication performance with minimum complexity. Each fog node must have issued the access permission for users' identities at letting user access method. Finding a technique that works in fog computing for rapid delegation

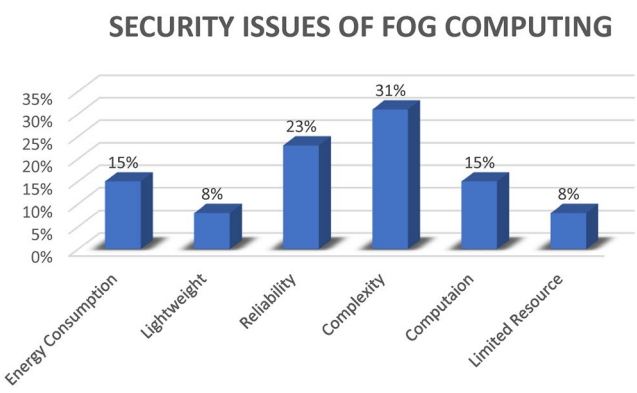

Fig. 8 Network security issues of fog computing

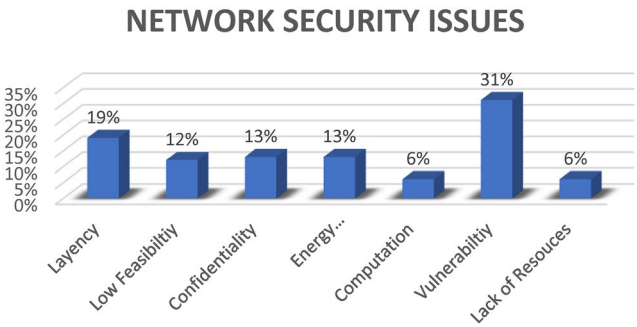

Fig. 9 Network security-based challenges

and authentication is problematic. We understand that the blockchain approaches utilized to improve sensor networks' efficiency through lightweight algorithms have been introduced in recent years. However, the efficient classification to detect attacks to prevent communication and fast performance is a major problem in fog computing. Thus, Artificial Intelligence and blockchain approaches can be combined [113–116] to achieve low latency, limited resources, low computation, and complexity to promote reliability in fog computing through intelligent contracts and learning approaches. Besides, the combined blockchain-based Artificial Intelligence methodology is utilized to improve the efficiency of the sensor network's detection of attacks in a reasonable timeframe. So, this combined methodology will be recommended to solve the vulnerability issue with network security. A research paper reported 31% of attack-based vulnerability problems [117]. Response time will grow, and numerous computing resources will be squandered if the protocols are insufficient.

Two major issues of the network are latency and attacks. Latency, cost, and energy consumption are resolved using a framework that combines fog computing with the security features offered by SDN and Artificial Intelligence [118, 119]. Since SDN technology has allowed such instructions to be propagated around the whole networking, cloud computing facilitates moving data centers closer to customers.

The fog nodes function to push changes across the network as regional decision-making components interacting with software-defined networking (SDN). Efficient decision-making and accurate recognition are performed to detect the attacks on the network by learning approaches.

5.3 Data Processing

When a large number of users are utilizing fog computing, each processing of data or information and distribution is challenging one in fog computing to its storage and resource availability. Database design is essential to allocate the optimum storage area for processing and deciding to reach the users. Besides, promoting data availability and confidentiality is essential when users distribute the data. Because of this, the authority processing the data in the real-time application is controlled. The information above encourages analyzing data security in fog computing. In this manner, efficient data processing relevant security issue analysis is provided according to the recent research approaches in this review paper. Data processing in fog computing is analyzed, including the merits and demerits of applications. The access control approach for efficient storage, novel software designing, and optimization algorithm for handling the redundant and excess data are used in data processing of fog computing. Besides, data security challenges, such as low availability of resources, data distribution speed, low detection of attacks, computation, cost, and latency, can be resolved using the recent approaches provided in Tables 9 and 10.

However, cloud services do not appropriately handle redundant data, illegal sharing of data, unauthorized access, and data altering. In addition, the difficulty of data security is presented in Fig. 10. According to that, and more attention is needed to developing user-friendly and efficient fog computing to achieve confidentiality, availability, and integrity in the data processing.

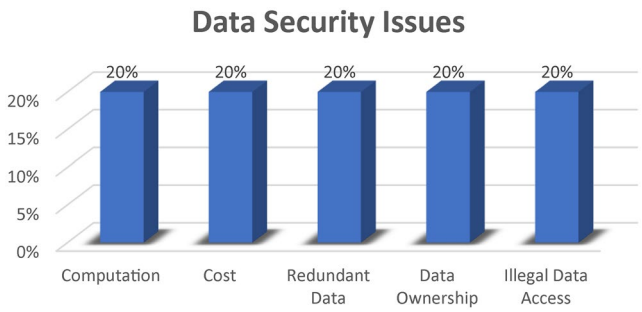

Fig. 10 Data security issues

5.4 Solution for Data Processing Challenges

The data processing of edge devices reduces fragmentation, resource use, and crucial data transmission amid IoT devices and a centralized fog system. Fog service providers, who act as a conduit between endpoint devices and cloud servers, are in charge of managing and configuring publicly available fog nodes. These nodes offer endpoint services that allow the processing, storing, and evaluation the data. SDN techniques provide efficient data processing and help to enhance the efficiency of data processing with minimum delay. As devices develop huge amounts of data, it becomes harder, demanding quick and effective data processing. So, the efficient optimization approach can be used to reduce the redundant data. Besides, the storage-based algorithm for data distribution in fog nodes is to be considerable for handle the large data. In addition, to enhance confidentiality, availability, and integrity, the blockchain technology can be used in fog computing to handle data effectively. Despite this, data ownership, computation, and cost ownership will be implemented using VANET combined with blockchain [120, 121].

5.5 Privacy–Based Security Analysis

The analysis of privacy security in fog computing has had a significant impact in recent years because the type of information sent to whom it is sent is decided by only the users, not the unauthorized user. It must apply to users and their activities when exchanging, gathering, transmitting, and processing sensitive data on fog nodes.

Privacy security for users and their locations has been considered in recent days. Issues such as latency, cost, location, and feasibility, reduce the quality of services in fog computing. In this manner, user and location privacy are discussed in this paper in Table 11. Based on this, the location privacy algorithm, encryption approach, lightweight false tolerance, and privacy-preserving scheme for energy preserving are provided to resolve the issues above in various IoT-based applications. The collected survey paper based on privacy issues is provided in Fig. 11.

Despite this, the lack of visibility and virtualization is a major problem in enhancing fog computing performance in privacy security. Specifically, lack of visibility increases vulnerability to security risks and makes it difficult to track down and fix performance issues. The lack of real-time data makes it impossible to see trends that point to emerging issues, which results in increased downtime and disruptions. In addition, location awareness is essential to avoid mutitendency.

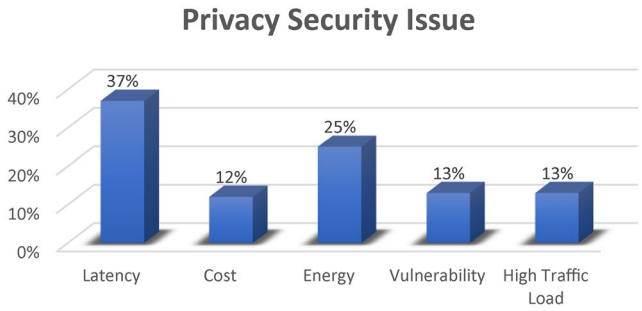

Fig. 11 Privacy issue of fog computing

5.6 Solution of Privacy Issues of Location and User

This study examined the issues of users and location privacy. Privacy is one of the users' significant concerns about their information in the fog for different reasons. The data from IoT devices in the physical world should be collected and encrypted to enhance data privacy during data transmission. As emphasized in the research, the most crucial feature of privacy is that the node location is concealed. In [122], a mechanism for disguising the location of automobiles on the online platform to accommodate fog from other networks is introduced. The research investigated multi-tendency and visibility issues of location and user privacy, which Artificial Intelligence and blockchain technologies can resolve. Specifically, AI effectively handles feature selection and recognition. Big data handling aids in the privacy restructuring for both the location and the user. Blockchain provides distributed database to securely keep a document or information to establish high-level security in fog computing [123–126].

6 Future Enhancement

Fog computing security continues to face evolving threats due to its distributed, resource-constrained, and heterogeneous nature. While existing approaches address several vulnerabilities, there remain critical gaps that future research should explore. Below, we outline concrete and actionable directions:

6.1 Lightweight AI for Fog Security

Resource limitations of fog nodes make heavy models impractical. Future work should investigate lightweight AI approaches such as TinyML for anomaly detection, federated learning for privacy-preserving training across distributed fog nodes, and reinforcement learning for adaptive threat response. These techniques can enhance real-time intrusion detection and reduce dependency on centralized cloud analysis.

6.2 Software-Defined Networking (SDN) for Dynamic Access Control

SDN offers programmability and centralized visibility that can complement fog's distributed architecture. Research should focus on implementing flow-based access control policies at fog gateways, enabling rapid mitigation of unauthorized access attempts. Dynamic SDN policies can also help balance latency, efficiency, and security, especially in time-sensitive applications such as healthcare and vehicular networks.

6.3 Lightweight Cryptographic Mechanisms

Fog devices demand security solutions that do not impose excessive computational or energy overhead. Future studies should examine lightweight encryption standards, elliptic curve cryptography (ECC), and post-quantum algorithms tailored for constrained devices. Benchmarking these schemes against fog-specific workloads would guide practical adoption.

6.4 Addressing Insider Threats and Trust Management

Insider threats remain underexplored in fog computing security. Novel frameworks integrating reputation-based trust systems and behavioral monitoring can help detect compromised fog nodes. Combining trust evaluation with decentralized consensus mechanisms (e.g., blockchain) could further strengthen resilience.

6.5 Quantitative and Temporal Security Analysis

Beyond qualitative surveys, future work should present quantitative metrics (e.g., percentage of studies addressing each vulnerability) and temporal trends in security research. Such analyses would highlight progress over time and identify underexplored areas requiring urgent attention.

7 Conclusion

In conclusion, fog computing represents a hierarchical architecture consisting of cloud–fog–device tiers. Unlike purely cloud-centric models, this hierarchy introduces a degree of decentralization by distributing resources and services closer to end-users, thereby reducing latency and improving responsiveness. This review has analyzed major

security challenges such as malware, node attacks, virtualization risks, and privacy concerns, while also evaluating mitigation techniques. The discussion highlights underexplored areas, including lightweight cryptographic methods, fog-specific insider threat detection, and advanced security mechanisms such as homomorphic encryption and blockchain-based authentication. Furthermore, future research directions—such as lightweight AI models for anomaly detection on resource-constrained devices and SDN-enabled dynamic access control—offer concrete pathways for enhancing fog security. Overall, while fog computing maintains a hierarchical structure, its partial decentralization provides significant opportunities to strengthen security and resilience in next-generation networks.

Author Contributions All authors have equal contribution.

Funding No.

Data Availability Data is available from the authors upon reasonable request.

Declarations

Ethical Approval This article does not contain any studies with human participants or animals performed by any of the authors.

Informed Consent Not applicable.

Conflict of Interest The authors declare that there is no conflict of interest regarding the publication of this paper.

References

1. Kaur K, Dhand T, Kumar N, Zeadally S (2017) Container-as-a-service at the edge: trade-off between energy efficiency and service availability at fog nano data centers. IEEE Wireless Commun 24(3):48–56. https://doi.org/10.1109/MWC.2017.1600427
2. Xu LD, He W, Li S (2014) Internet of things in industries: a survey. IEEE Trans Ind Inf 10(4):2233–2243. https://doi.org/10.1109/TII.2014.2300753
3. Baliga J, Ayre RWA, Hinton K, Tucker RS (2011) Green cloud computing: balancing energy in processing, storage, and transport. Proc IEEE 99(1):149–167. https://doi.org/10.1109/JPROC.2010.2060451
4. Singh J, Singh P, Gill SS (2021) Fog computing: a taxonomy, systematic review, current trends and research challenges. J Parallel Distrib Comput 157:56–85. https://doi.org/10.1016/j.jpdc.2021.06.005
5. Yousefpour A et al (2019) All one needs to know about fog computing and related edge computing paradigms: a complete survey. J Syst Archit 98:289–330. https://doi.org/10.1016/j.sysarc.2019.02.009
6. Maiti P, Apat HK, Sahoo B, Turuk AK (2019) An effective approach of latency-aware fog smart gateways deployment for IOT services. Internet Things 8:100091. https://doi.org/10.1016/j.iot.2019.100091
7. Wöbker C, Seitz A, Mueller H, Bruegge B (2018) Fogernetes: deployment and management of fog computing applications. In: NOMS 2018 – 2018 IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, 1–7. https://doi.org/10.1109/NOMS.2018.8406321
8. Habibi P, Farhoudi M, Kazemian S, Khorsandi S, Leon-Garcia A (2020) Fog computing: a comprehensive architectural survey. IEEE Access 8:69105–69133. https://doi.org/10.1109/ACCESS.2020.2983253
9. Byers CC (2017) Architectural imperatives for fog computing: use cases, requirements, and architectural techniques for fog-enabled IoT networks. IEEE Commun Mag 55(8):14–20. https://doi.org/10.1109/MCOM.2017.1600885
10. Mutlag AA, Abd Ghani MK, Arunkumar N, Mohammed MA, Mohd O (2019) Enabling technologies for fog computing in healthcare IOT systems. Futu Gene Com Sys 90:62–78. https://doi.org/10.1016/j.future.2018.07.049
11. Tayeb S, Latifi S, Kim Y (2017) A survey on IoT communication and computation frameworks: an industrial perspective. In: 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, pp 1–6. https://doi.org/10.1109/CCWC.2017.7868354
12. Tuli S, Mahmud R, Tuli S, Buyya R (2019) FogBus: a blockchain-based lightweight framework for edge and fog computing. J Syst Softw 154:22–36. https://doi.org/10.1016/j.jss.2019.04.050
13. Khan G, Gola KK, Kanauzia R, Kumar S (2022) Secure architecture to support IOT based on fog computing. Proc Comp Sci 215:608–617. https://doi.org/10.1016/j.procs.2022.12.063
14. Shabu SS et al (2022) Trajectory clustering and query processing analysis framework for knowledge discovery in cloud environment. Expert Systems 40(4). https://doi.org/10.1111/exsy.12968
15. Costa B, Bachiega J, Carvalho LR, Rosa M, Araujo A (2022) Monitoring fog computing: a review, taxonomy and open challenges. Comput Networks 215:109189. https://doi.org/10.1016/j.comnet.2022.109189
16. Alazab M, Rm SP, M P, Maddikunta PKR, Gadekallu TR, Pham Q-V (2022) Federated learning for Cybersecurity: concepts, challenges, and future directions. IEEE Trans Ind Inf 18(5):3501–3509. https://doi.org/10.1109/TII.2021.3119038
17. Laghari AA, Jumani AK, Laghari RA (2021) Review and state of art of fog computing. Archives Comput Methods Eng 28(5):3631–3643. https://doi.org/10.1007/s11831-020-09517-y
18. Rani R, Kumar N, Khurana M, Kumar A, Barnawi A (2021) Storage as a service in fog computing: a systematic review. J Syst Archit 116:102033. https://doi.org/10.1016/j.sysarc.2021.102033
19. Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B (2019) A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access 7:82721–82743. https://doi.org/10.1109/ACCESS.2019.2924045

20. Naha RK et al (2018) Fog computing: survey of trends, architectures, requirements, and research directions. IEEE Access 6:47980–48009. https://doi.org/10.1109/ACCESS.2018.2866491
21. Kaur J, Kumar R, Agrawal A, Khan RA (2022) A neutrosophic AHP-based computational technique for security management in a fog computing network. J Sport Hist Supercomput 79(1):295–320. https://doi.org/10.1007/s11227-022-04674-2
22. Waqas M et al (2023) Defense scheme against advanced persistent threats in mobile fog computing security. Comput Networks 221:109519. https://doi.org/10.1016/j.comnet.2022.109519
23. Namane S, Ahmim M, Kondoro A, Dhaou IB (2023) Blockchain-based authentication scheme for collaborative traffic light systems using fog computing. Electronics 12(2):431. https://doi.org/10.3390/electronics12020431
24. Azizpour S, Majma M (2022) Nada: new architecture for detecting DOS and ddos attacks in fog computing. J Comput Virol Hacking Tech 19(1):51–64. https://doi.org/10.1007/s11416-022-00431-4
25. Chakraborty C, Othman SB, Almalki FA, Sakli H (2023) FC-Seeda: fog computing-based secure and energy efficient data aggregation scheme for internet of healthcare things. Neural Comput Appl. https://doi.org/10.1007/s00521-023-08270-0
26. Khanagha S, Ansari S, Paroutis S, Oviedo L (2020) Mutualism and the dynamics of new platform creation: a study of Cisco and fog computing. Strateg Manag J 43(3):476–506. https://doi.org/10.1002/smj.3147
27. Mohammed A (2019) Fog computing complementary approach to cloud computing. SSRN Electron J. https://doi.org/10.2139/ssrn.3660962
28. Sharma V, Gola KK (2016) ASCCS: architecture for secure communication using cloud services. Adv Intell Syst Comput 19–25. https://doi.org/10.1007/978-981-10-0451-3_3
29. Vaquero LM, Rodero-Merino L (2014) Finding your way in the fog. ACM SIGCOMM Comput Commun Rev 44(5):27–32. https://doi.org/10.1145/2677046.2677052
30. Yang Y, Luo X, Chu X, Zhou M-T (2019) Fog computing architecture and technologies In: Fog-Enabled Intelligent IoT Systems pp 39–60. https://doi.org/10.1007/978-3-030-23185-9_2
31. Ema RR, Islam T, Ahmed MH (2019) Suitability of using fog computing alongside cloud computing. In: 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, pp 1–4. https://doi.org/10.1109/ICCCNT45670.2019.8944906
32. Ahuja SP, Wheeler N (2020) Architecture of FOG-enabled and cloud-enhanced internet of things applications. Int J Multiling Cloud Appl Comput 10(1):1–10. https://doi.org/10.4018/ijcac.2020010101
33. Mahmud R, Kotagiri R, Buyya R (2017) Fog computing: a taxonomy, survey and future directions. In: Internet of Things pp 103–130. https://doi.org/10.1007/978-981-10-5861-5_5
34. Sehgal VK, Patrick A, Soni A, Rajput L (2015) Smart human security framework using internet of things, cloud and fog computing. Intell Distrib Comput 251–263. https://doi.org/10.1007/978-3-319-11227-5_22
35. H S, V N (2021) A review on fog computing: architecture, fog with IOT, algorithms and research challenges. ICT Express 7(2):162–176. https://doi.org/10.1016/j.icte.2021.05.004
36. Atlam H, Walters R, Wills G (2018) Fog computing and the internet of things: a review. Big Data Cognit Comput 2(2):10. https://doi.org/10.3390/bdcc2020010
37. Das R, Inuwa MM (2023) A review on fog computing: issues, characteristics, challenges, and potential applications. Telematics Inf Rep 10:100049. https://doi.org/10.1016/j.teler.2023.100049
38. Mollah MB, Islam KR, Islam SS (2012) Next generation of computing through cloud computing technology. In: 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), vol 2012, Montreal, QC, Canada, pp 1–6. https://doi.org/10.1109/CCECE.2012.6334973
39. Chen B, Wan J, Celesti A, Li D, Abbas H, Zhang Q (2018) Edge computing in IoT-based manufacturing. IEEE Commun Mag 56(9):103–109. https://doi.org/10.1109/MCOM.2018.1701231
40. Tawalbeh L, Jararweh Y, Ababneh F, Dosari F (2015) Large scale cloudlets deployment for efficient mobile cloud computing. J Retail 10(1). https://doi.org/10.4304/jnw.10.01.70-76
41. Barbarossa S, Sardellitti S, Di Lorenzo P (2014) Communicating while computing: distributed mobile cloud computing over 5G heterogeneous networks. IEEE Signal Process Mag 31(6):45–55. https://doi.org/10.1109/MSP.2014.2334709
42. Rashid Abdulqadir H et al (2021) A study of moving from cloud computing to fog computing. Qubahan Acad J 1(2):60–70. https://doi.org/10.48161/qaj.v1n2a49
43. Dolui K, Datta SK (2017) Comparison of edge computing implementations: fog computing, cloudlet and mobile edge computing. In: 2017 Global Internet of Things Summit (GIoTS), Geneva, Switzerland pp 1–6. https://doi.org/10.1109/GIOTS.2017.8016213
44. Peralta G, Iglesias-Urkia M, Barcelo M, Gomez R, Moran A, Bilbao J (2017) Fog computing based efficient IoT scheme for the industry 4.0. In: 2017 IEEE International Workshop of Electronics, Control, Measurement, Signals and their Application to Mechatronics (ECMSM), Donostia, Spain, pp 1–6. https://doi.org/10.1109/ECMSM.2017.7945879
45. Ben Hassen H, Ayari N, Hamdi B (2020) A home hospitalization system based on the internet of things, fog computing and cloud computing. Inf Med Unlocked 20:100368. https://doi.org/10.1016/j.imu.2020.100368
46. Javadzadeh G, Rahmani AM (2019) Fog computing applications in smart cities: a systematic survey. Wireless Networks 26(2):1433–1457. https://doi.org/10.1007/s11276-019-02208-y
47. Wang Y, Uehara T, Sasaki R (2015) Fog computing: issues and challenges in security and forensics. In: 2015 IEEE 39th Annual Computer Software and Applications Conference, Taichung, Taiwan, 53–59. https://doi.org/10.1109/COMPSAC.2015.173
48. Zhang P, Zhou M, Fortino G (2018) Security and trust issues in fog computing: a survey. Futu Gene Com Sys 88:16–27. https://doi.org/10.1016/j.future.2018.05.008
49. Ometov A, Molua OL, Komarov M, Nurmi J (2022) A survey of security in cloud, edge, and fog computing. Sensors 22(3):927. https://doi.org/10.3390/s22030927
50. Yi S, Li C, Li Q (2015) A survey of fog computing. In: Proceedings of the 2015 Workshop on Mobile Big Data. https://doi.org/10.1145/2757384.2757397
51. Zhou C, Fu A, Yu S, Yang W, Wang H, Zhang Y (2020) Privacy-preserving federated learning in fog computing. IEEE Internet Things J 7(11):10782–10793. https://doi.org/10.1109/JIOT.2020.2987958
52. Osanaiye O et al (2017) From cloud to fog computing: a review and a conceptual live VM migration framework. IEEE Access 5:8284–8300. https://doi.org/10.1109/access.2017.2692960
53. Alhumam NA, Alyemni NS, Hafizur Rahman MM (2023) Cyber security in fog computing using blockchain: a mini literature review. In: 2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC). https://doi.org/10.1109/icaiic57133.2023.10066994
54. Gu K, Wu N, Yin B, Jia W (2020) Secure data query framework for cloud and fog computing. IEEE Trans Network Service Manag 17(1):332–345. https://doi.org/10.1109/TNSM.2019.2941869
55. Mukherjee M et al (2017) Security and privacy in fog computing: challenges. IEEE Access 5:19293–19304. https://doi.org/10.1109/ACCESS.2017.2749422

56. Laroui M et al (2021) Edge and fog computing for IOT: a survey on current research activities & future directions. Comput Commun 180:210–231. https://doi.org/10.1016/j.comcom.2021.09.003
57. Kalaria R, Kayes ASM, Rahayu W, Pardede E (2021) A secure mutual authentication approach to fog computing environment. Comput Secur 111:102483. https://doi.org/10.1016/j.cose.2021.102483
58. Mohammed S, L R, V R R (2017) Password-based authentication in Computer security: why is it still there? SIJ Trans Comput Sci Eng Appl 5(3):01–05. https://doi.org/10.9756/sijcsea/v5i3/05010060101
59. Asha HP, Jingle ID (2022) One time password-based two channel authentication mechanism using blockchain. Data Sci Secur 229–237. https://doi.org/10.1007/978-981-19-2211-4_20
60. Amin R, Kunal S, Saha A, Das D, Alamri A (2020) CFSEC: password based secure communication protocol in cloud-fog environment. J Parallel Distrib Comput 140:52–62. https://doi.org/10.1016/j.jpdc.2020.02.005
61. Zhang H, Qin B, Tu T, Guo Z, Gao F, Wen Q (2020) An adaptive encryption-as-a-service architecture based on fog computing for real-time substation communications. IEEE Trans Ind Inf 16(1):658–668. https://doi.org/10.1109/TII.2019.2948113
62. Viriyasitavat W, Da Xu L, Dhiman G, Sapsomboon A, Pungpapong V, Bi Z (2023) Service workflow: state-of-the-art and future trends. IEEE Trans Serv Comput 16(1):757–772. https://doi.org/10.1109/TSC.2021.3121394
63. Kakei S, Shiraishi Y, Saito S (2021) Simplifying dynamic public key certificate graph for certification path building in distributed public key infrastructure. In: 2021 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, pp 545–550. https://doi.org/10.1109/ICTC52510.2021.9620853
64. Amanlou S, Hasan MK, Bakar KA (2021) Lightweight and secure authentication scheme for IOT network based on publish–subscribe fog computing model. Comput Networks 199:108465. https://doi.org/10.1016/j.comnet.2021.108465
65. Tehranipoor F, Karimian N, Yan W, Chandy JA (2017) Dram-based intrinsic physically unclonable functions for system-level security and authentication. IEEE Trans VLSI Syst 25(3):1085–1097. https://doi.org/10.1109/tvlsi.2016.2606658
66. Guo Y, Guo Y (2021) Fogha: an efficient handover authentication for mobile devices in fog computing. Comput Secur 108:102358. https://doi.org/10.1016/j.cose.2021.102358
67. Umoren O, Singh R, Pervez Z, Dahal K (2022) Securing fog computing with a decentralised user authentication approach based on blockchain. Sensors 22(10):3956. https://doi.org/10.3390/s22103956
68. Ahmadi F, Sonia, Gupta G, Zahra SR, Baglat P, Thakur P (2021) Multi-factor biometric authentication approach for fog computing to ensure security perspective. In: 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, pp 172–176
69. Chatterjee S, Roy S, Das AK, Chattopadhyay S, Kumar N, Vasilakos AV (2018) Secure biometric-based authentication scheme using Chebyshev chaotic Map for multi-server environment. IEEE Trans Intell Transp Syst Dependable Secure Comput 15(5):824–839. https://doi.org/10.1109/TDSC.2016.2616876
70. Zhang P, Liu JK, Yu FR, Sookhak M, Au MH, Luo X (2018) A survey on access control in fog computing. IEEE Commun Mag 56(2):144–149. https://doi.org/10.1109/MCOM.2018.1700333
71. Gungor VC, Hancke GP (2009) Industrial wireless sensor networks: challenges, design principles, and technical approaches. IEEE Trans Ind Electron 56(10):4258–4265. https://doi.org/10.1109/TIE.2009.2015754
72. Salonikias S, Mavridis I, Gritzalis D (2016) Access control issues in utilizing fog computing for transport infrastructure. In: Critical Information Infrastructures Security pp 15–26. https://doi.org/10.1007/978-3-319-33331-1_2
73. Cannady J, Jay H (1996) A comparative analysis of current intrusion detection technologies. In: Proceedings of the Fourth Technology for Information Security Conference, vol 96
74. Servos D, Osborn SL (2017) Current research and open problems in attribute-based access control. ACM Comput Surv 49(4):1–45. https://doi.org/10.1145/3007204
75. Haddouti SE, Kettani MD (2022) A secure and trusted fog computing approach based on blockchain and identity federation for a granular access control in IOT environments. Int J Advan Comput Sci Appl 13(3). https://doi.org/10.14569/ijacsa.2022.0130368
76. Liu M, Yang C, Li H, Zhang Y (2020) An efficient attribute-based access control (ABAC) policy retrieval method based on attribute and value levels in multimedia networks. Sensors 20(6):1741. https://doi.org/10.3390/s20061741
77. Liu F, Tang Y, Wang L (2019) EHAPAC: a privacy-supported access control model for IP-enabled wireless sensor networks. Sensors 19(7):1513. https://doi.org/10.3390/s19071513
78. Li S, Ren W, Zhu T, Choo K-KR (2018) Lico: a lightweight access control model for inter-networking linkages. IEEE Access 6:51748–51755. https://doi.org/10.1109/ACCESS.2018.2870148
79. Vohra K, Dave M (2018) Multi-authority attribute based data access control in fog computing. Proc Comp Sci 132:1449–1457. https://doi.org/10.1016/j.procs.2018.05.078
80. R. K, S. SM, M SK (2017) Pre-channel scheduling and priority-based reservation in medium access control for industrial wireless sensor network applications. Comput Electr Eng 64:322–336. https://doi.org/10.1016/j.compeleceng.2017.05.010
81. Downs DD, Rub JR, Kung KC, Jordan CS (1985) Issues in discretionary access control. In: 1985 IEEE Symposium on Security and Privacy, Oakland, CA, USA, pp 208–208. https://doi.org/10.1109/SP.1985.10014
82. Almehmadi A, El-Khatib K (2017) On the possibility of insider threat prevention using intent-based access control (IBAC). IEEE Syst J 11(2):373–384. https://doi.org/10.1109/JSYST.2015.2424677
83. Thomas RK, Sandhu RS (1998) Task-based authorization controls (TBAC): a family of models for active and enterprise-oriented authorization management. In: Database Security XI, pp 166–181. https://doi.org/10.1007/978-0-387-35285-5_10
84. Desai S, Vyas T, Jambekar V (2020) Security and privacy issues in fog computing for healthcare 4.0. In: Fog Computing for Healthcare 4.0 Environments, pp 291–314. https://doi.org/10.1007/978-3-030-46197-3_12
85. Mohamed I, Al-Mahdi H, Tahoun M, Nassar H (2022) Characterization of task response time in fog enabled networks using queueing theory under different virtualization modes. J Cloud Comput 11(1). https://doi.org/10.1186/s13677-022-00293-7
86. Rahman FH et al (2022) Entruve: energy and trust-aware virtual machine allocation in vehicle fog computing for catering applications in 5G. Futu Gene Com Sys 126:196–210. https://doi.org/10.1016/j.future.2021.07.036
87. Li Q, Zhao L, Gao J, Liang H, Zhao L, Tang X (2018) SMDP-Based coordinated virtual machine allocations in cloud-fog computing systems. IEEE Internet Things J 5(3):1977–1988. https://doi.org/10.1109/JIOT.2018.2818680
88. Luo J et al (2019) Container-based fog computing architecture and energy-balancing scheduling algorithm for energy IOT. Futu Gene Com Sys 97:50–60. https://doi.org/10.1016/j.future.2018.12.063
89. Kang J, Yu H (2018) Mitigation technique for performance degradation of virtual machine owing to GPU pass-through in fog

computing. J Commun Networks 20(3):257–265. https://doi.org/10.1109/jcn.2018.000038
90. Pang J, Yang S, He L, Chen Y, Ren N (2019) Intelligent control/operational strategies in WWTPS through an integrated Q-learning algorithm with ASM2D-guided reward. Water 11(5):927. https://doi.org/10.3390/w11050927
91. Sadaf K, Sultana J (2020) Intrusion detection based on autoencoder and isolation forest in fog computing. IEEE Access 8:167059–167068. https://doi.org/10.1109/ACCESS.2020.3022855
92. Shafi Q, Basit A, Qaisar S, Koay A, Welch I (2018) Fog-assisted SDN controlled framework for enduring anomaly detection in an IoT network. IEEE Access 6:73713–73723. https://doi.org/10.1109/ACCESS.2018.2884293
93. Daoud WB, Obaidat MS, Meddeb-Makhlouf A, Zarai F, Hsiao K-F (2019) TACRM: trust access control and resource management mechanism in fog computing. Hum Cent Comput Inf Sci 9(1). https://doi.org/10.1186/s13673-019-0188-3
94. Fang W, Zhang W, Chen W, Liu Y, Tang C (2019) TMSRS: trust management-based secure routing scheme in industrial wireless sensor network with fog computing. Wireless Networks 26(5):3169–3182. https://doi.org/10.1007/s11276-019-02129-w
95. Rahman FH, Newaz SHS, Au TW, Suhaili WS, Lee GM (2020) Off-street vehicular fog for catering applications in 5G/B5G: a trust-based task mapping solution and open research issues. IEEE Access 8:117218–117235. https://doi.org/10.1109/ACCESS.2020.3004738
96. Kouicem DE, Imine Y, Bouabdallah A, Lakhlef H (2022) Decentralized blockchain-based trust management protocol for the internet of things. IEEE Trans Intell Transp Syst Dependable Secure Comput 19(2):1292–1306. https://doi.org/10.1109/TDSC.2020.3003232
97. Narendra NC, Koorapati K, Ujja V (2015) Towards cloud-based decentralized storage for Internet of Things data. In: 2015 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), Bangalore, India, 160–168. https://doi.org/10.1109/CCEM.2015.9
98. Vasconcelos DR, Severino VS, Maia MEF, de Castro Andrade RM, de Souza JN (2018) Bio-inspired model for data distribution in fog and Mist computing. In: 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, pp 777–782. https://doi.org/10.1109/COMPSAC.2018.10336
99. Linaje M, Berrocal J, Galan-Benitez A (2019) Mist and edge storage: fair storage distribution in sensor networks. IEEE Access 7:123860–123876. https://doi.org/10.1109/ACCESS.2019.2938443
100. Gowda NC, Manvi SS, A. BM, Lorenz P (2023) BSKM-FC: Blockchain-based secured key management in a fog computing environment. Futu Gene Com Sys 142:276–291. https://doi.org/10.1016/j.future.2022.12.042
101. Huang Q, Yang Y, Wang L (2017) Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things. IEEE Access 5:12941–12950. https://doi.org/10.1109/ACCESS.2017.2727054
102. Sánchez-Gallegos DD et al (2020) On the continuous processing of health data in edge-fog-cloud computing by using micro/nanoservice composition. IEEE Access 8:120255–120281. https://doi.org/10.1109/ACCESS.2020.3006037
103. Thakkar HK, Sahoo PK (2022) IOT based ECG-SCG big data analysis framework for continuous cardiac health monitoring in cloud data centers. In: Predictive Analytics in Cloud, Fog, and Edge Computing, pp 177–184. https://doi.org/10.1007/978-3-031-18034-7_10
104. Mohammed BA et al (2023) Anaa-fog: a novel anonymous authentication scheme for 5G-enabled vehicular fog computing. Mathematics 11(6):1446. https://doi.org/10.3390/math11061446
105. Chen S, Zhu X, Zhang H, Zhao C, Yang G, Wang K (2020) Efficient privacy preserving data collection and computation offloading for fog-assisted IoT. IEEE Trans Sustain Comput 5(4):526–540. https://doi.org/10.1109/TSUSC.2020.2968589
106. Feng J, Yang LT, Zhang R, Qiang W, Chen J (2022 Oct) Privacy preserving high-order bi-lanczos in cloud–fog computing for industrial applications. IEEE Trans Ind Inf 18(10):7009–7018. https://doi.org/10.1109/TII.2020.2998086
107. Li M, Zhu L, Lin X (2019) Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing. IEEE Internet Things J 6(3):4573–4584. https://doi.org/10.1109/JIOT.2018.2868076
108. Naik C, Siddhartha M, Martin JP, Chandrasekaran K (2019) Location privacy using data obfuscation in fog computing. In: TENCON 2019 – 2019 IEEE Region 10 Conference (TENCON), Kochi, India, pp 1286–1291. https://doi.org/10.1109/TENCON.2019.8929236
109. Zheng L, Yue H, Li Z, Pan X, Wu M, Yang F (2018) K-anonymity location privacy algorithm based on clustering. IEEE Access 6:28328–28338. https://doi.org/10.1109/ACCESS.2017.2780111
110. Li G, Zhang Q, Li J, Wu J, Zhang P (2018) Energy-efficient location privacy preserving in vehicular networks using social intimate fogs. IEEE Access 6:49801–49810. https://doi.org/10.1109/ACCESS.2018.2859344
111. Boualouache A, Sedjelmaci H, Engel T (2021) Consortium blockchain for cooperative location privacy preservation in 5G-enabled vehicular fog computing. IEEE Trans Veh Technol 70(7):7087–7102. https://doi.org/10.1109/TVT.2021.3083477
112. Nguyen Gia T, Nawaz A, Peña Querata J, Tenhunen H, Westerlund T (2020) Artificial intelligence at the edge in the blockchain of things In: Lecture Notes of the Institute for Computer Sciences. Soc Inf Telecommun Eng 267–280. https://doi.org/10.1007/978-3-030-49289-2_21
113. Kochovski P, Gec S, Stankovski V, Bajec M, Drobintsev PD (2019) Trust management in a blockchain based fog computing platform with trustless smart oracles. Futu Gene Com Sys 101:747–759. https://doi.org/10.1016/j.future.2019.07.030
114. Luong NC, Jiao Y, Wang P, Niyato D, Kim DI, Han Z (2020) A machine-learning-based auction for resource trading in fog computing. IEEE Commun Mag 58(3):82–88. https://doi.org/10.1109/MCOM.001.1900136
115. Kumar P, Kumar R, Gupta GP, Tripathi R (2020) A distributed framework for detecting DDOS attacks in smart contract-based blockchain-IoT systems by leveraging fog computing. Trans Emerging Telecommun Technol 32(6). https://doi.org/10.1002/ett.4112
116. Tu S et al (2018) Security in fog computing: a novel technique to tackle an impersonation attack. IEEE Access 6:74993–75001. https://doi.org/10.1109/ACCESS.2018.2884672
117. Ghosh S, Chandra V, Adhya A (2021) Machine learning for fog computing-based IoT networks in smart city environment. In: Internet of Things pp 267–285. https://doi.org/10.1007/978-3-030-81473-1_13
118. Alotaibi J, Alazzawi L (2021) SaFIoV: a secure and fast communication in fog-based internet-of-vehicles using SDN and blockchain. In: 2021 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS), Lansing, MI, USA, pp 334–339. https://doi.org/10.1109/MWSCAS47672.2021.9531857
119. Jiao Y, Wang P, Niyato D, Suankaewmanee K (2019) Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks. IEEE Trans Parallel Distrib Syst 30(9):1975–1989. https://doi.org/10.1109/TPDS.2019.2900238

120. Shynu G, Menon VG, Kumar RL, Kadry S, Nam Y (2021) Blockchain-based secure healthcare application for diabetic-cardio disease prediction in fog computing. IEEE Access 9:45706–45720. https://doi.org/10.1109/ACCESS.2021.3065440
121. Gao J et al (2020) A blockchain-SDN-Enabled Internet of vehicles environment for fog computing and 5G networks. IEEE Internet Things J 7(5):4278–4291. https://doi.org/10.1109/JIOT.2019.2956241
122. Sharma PK, Chen M-Y, Park JH (2018) A software defined fog node based distributed blockchain cloud architecture for IoT. IEEE Access 6:115–124. https://doi.org/10.1109/ACCESS.2017.2757955
123. Kong Q, Su L, Ma M (2021) Achieving privacy-preserving and verifiable data sharing in vehicular fog with blockchain. IEEE Trans Intell Transp Syst 22(8):4889–4898. https://doi.org/10.1109/TITS.2020.2983466
124. Kumar P et al (2021) PPSF: a privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities. IEEE Trans Network Sci Eng 8(3):2326–2341. https://doi.org/10.1109/TNSE.2021.3089435
125. Kumar R, Kumar P, Tripathi R, Gupta GP, Kumar N, Hassan MM (2022) A privacy-preserving-based secure framework using blockchain-enabled deep-learning in cooperative intelligent transport system. IEEE Trans Intell Transp Syst 23(9):16492–16503. https://doi.org/10.1109/TITS.2021.3098636
126. Hewa T, Braeken A, Liyanage M, Ylianttila M (2022) Fog computing and blockchain-based security service architecture for 5G industrial IoT-enabled cloud manufacturing. IEEE Trans Ind Inf 18(10):7174–7185. https://doi.org/10.1109/TII.2022.3140792