World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(Research Article)

Check for updates

Privacy and security issues in fog-to-fog communication: A survey

Timothy Murkomen *

Department of Computer Science and Software Engineering – School of Informatics and Innovative Systems; Jaramogi Oginga Odinga University of Science and Technology (JOOUST); P.O Box 210-Bondo.

World Journal of Advanced Research and Reviews, 2023, 20(03), 466–491

Publication history: Received on 27 October 2023; revised on 04 December 2023; accepted on 06 December 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.20.3.2487

Abstract

The rapid growth of Fog Computing has brought a paradigm shift in data processing and communication, presenting various benefits such as reduced latency, efficient data processing, enhanced scalability and the ability to operate effectively in resource-constrained environments. However, the technology introduced complex privacy and security issues. This paper conducted a thorough exploration of privacy and security issues associated with fog-to-fog (F2F) communication within the broader framework of fog computing. It initiated by providing a background of fog computing, it's architecture and the core characteristics of fog computing. This survey aimed to discuss the state-of-the-art of privacy and security concerns in fog-to-fog communication. The survey also proposed the areas of future research to equip researchers, practitioners, policy makers and the decision makers with solid knowledge, offering guidance in navigating the complex landscape of privacy and security issues in fog-to-fog (F2F) communication. The survey also aimed to discuss the existing privacy and security research gaps in fog-to-fog (F2F) communication. The findings of this review underscore privacy and security issues in F2F communication, providing valuable insights into recommended countermeasures to strengthen the overall security framework.

Keywords: Fog Computing; F2F; Privacy; Security; Fog-to-Fog Communication; Internet of Things (IoT); Cloud Computing; Artificial Intelligence; AI

1. Introduction

Fog Computing refers to extending cloud services to edge computing [1]. It's a concept of distributed computing and its main aim is to simplify the processing and configuration of computing ecosystem and storage devices between the end points and the data centres [2]. This exchange of data between fog nodes has revolutionized data processing and real time data processing. The Internet of Things (IoT) computational operations such as data analysis are executed by utilizing the distributed computing infrastructure – the Fog Computing. [3], [4]. Internet of Things (IoT) functions as an intelligence engine, enabling the acquisition of vast and huge data and facilitating automation across various domains. [5], [6]. The devices in IoT rely on cloud infrastructure to enhance the adaptability, ensure the systems are stable, bolster fault tolerance and facilitate more communications [7], [8], [9], and because of the huge expansion of these IoT devices [10], the cloud handles huge sensitive data, Fog computing was then proposed to overcome the problems of cloud computing [11]. When fog-enabled devices are in operation, they perform local assessments of time-sensitive data, including alarm statuses, device conditions, fault alerts, and other critical information [12], [13].

This architecture brings numerous advantages, including reduced latency [14], [15], enhanced real-time capabilities, and efficient bandwidth utilization. However, as fog computing escalates to meet the ever growing demands of various applications, from IoT, VANETs, smart cities, industrial automation, and healthcare, it also brings the concern of privacy and security issues. Fog computing introduces a decentralized computing paradigm that challenges the traditional security models that relied mostly on centralized controls [16]-[20]. The proximity of these computing resources closer

* Corresponding author: Timothy Murkomen

to the edge raises questions about how data security and privacy can be ensured. Ensuring secure and dependable communication is imperative in addressing the challenges posed by the ever-evolving environment [21], [22]. The presence of vast amounts of data underscores the need for real-time solutions, a requirement that can be fulfilled by integrating cloud computing technologies into IoT networks [23], [24].

In this paper, a detailed examination of the privacy and security issues [25] in fog computing more specifically to fog-to-fog communication. The survey aims to offer an in-depth understanding on fog-to-fog communication and the potential privacy and security issues in fog-to-fog communication. To achieve the survey's objective, we begin by presenting the general overview of fog computing and its impact in addressing privacy and security concerns in cloud computing arena. We will examine the general characteristics of fog computing, its benefits and explore their relevance in privacy and security issues within the realm of cloud computing. The paper also analyzes proposed solutions that address the privacy and security concerns in the field of cloud computing.

The findings of the paper will contribute immensely to the existing body of knowledge by equipping researchers, practitioners, policy makers and decision-makers with valuable insights in privacy and security issues in fog computing while offering a roadmap for navigating these critical concerns and fostering the responsible deployment of this technology. This knowledge will help inform research and development of very robust frameworks to address and support the improvements of trustworthy and secure fog-to-fog communication that prioritizes data protection.

This survey paper makes significant contributions:

1.1. Contextualizing Fog Computing

The paper provides a comprehensive overview of fog computing explaining its role in extending cloud services and simplifying the processing and storage of data between end points.

1.2. Privacy and security issues in fog-to-fog communication

The paper delves into the core focus of the survey, which is the privacy and security issues in fog-to-fog communication.

1.3. Countermeasures to privacy and security issues in fog-to-fog communication

The paper also discusses insightful countermeasures of privacy and security issues in fog-to-fog communication.

1.4. Open research gaps in fog-to-fog communication

The paper outlines open research gaps in privacy and security issues in fog-to-fog communication.

The paper is enumerated as follows: Section I and II provides a concise introduction and overview of key concepts related to fog computing including its architecture. Section III conducts a comprehensive survey of the relevant literature and other related work. Section IV outlines the methodology adopted for this survey paper. Section V presents the findings and analysis derived from the study. Section VI presents an in-depth exploration of the existing body of knowledge of Fog-to-Fog Communication. Section VII offers a comprehensive discussion of the findings. Section VIII presents open research gaps and future direction and finally the concluding remarks of this review paper.

2. Motivation

The motivation behind conducting this survey lies in the high escalation of Internet of Things (IoT) devices and increasing high demand for real-time data processing and the critical need to address privacy and security concerns within fog computing ecosystem. Fog Computing focuses on real-time data processing and increased adoption in applications like Internet of Things (IoT), Vehicular Ad hoc Networks (VANETs), smart cities, smart contracts and industrial automation. Understanding and mitigating these privacy and security issues will guide practitioners, researchers and all stakeholders in ensuring data protection and trust in this rapidly evolving landscape of fog computing.

2.1. Overview of Fog Computing

Fog Computing was formally introduced by Cisco as an extension of cloud computing which is close to the IoT devices in a network [26]. Cloud computing has many benefits including high valuable and efficient computing resources with an affordable price [27]-[30]. According to [31], numerous cloud services are readily accessible in contemporary commercial offerings; however, they may not be well-suited for addressing latency and portability requirements.

Examples of such applications include Wearable Computing, Smart Grids, Connected Vehicles [32] and Software Defined Networks (SDN) [33]. Fog aims to provide a decentralized computing paradigm that particularly extends the capabilities of cloud computing [34] as shown in Fig 1. The architecture processes, aggregates and transmit data hence saving time and resources.

2.2. Fog Computing Architecture

In this section, we discuss the architectural framework of fog computing. Given that a multitude of data originates from edge devices, sensors [35], and applications on a daily basis, it is imperative to acknowledge that these data-producing devices are typically characterized by simplicity and limited computational resources, rendering them ill-equipped to undertake essential analytics or machine-learning tasks [36]-[39]. Cloud computing offers robust capabilities for managing computing tasks. However, its distance can result in latency issues. Connecting endpoints directly to the cloud isn't viable due to privacy, security, and legal concerns associated with transmitting raw data over the internet. [40].

In Fog Computing, we look at the "fog" layer from the point of view of devices like gateways, routers, and others [41]. This "fog" layer is like a middle step that helps limit the data sent to the cloud and makes decisions based on specific rules programmed into the fog node. Fog Computing is used in different fields like industrial IoT, vehicle networks, smart cities, and smart buildings [42] as shown in Fig 2 below.

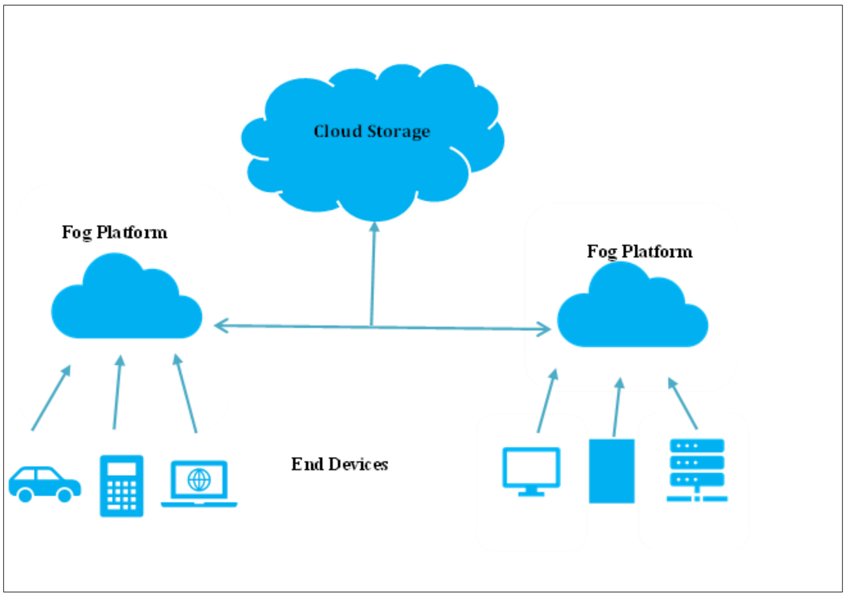

Figure 1 Fog Computing Overview

2.3. Characteristics of Fog Computing

The characteristics of fog computing makes it a valuable paradigm for applications requiring low latency [43], real-time processing, and distributed computing, such as IoT, smart cities, and automation. It is characterized by several key features [44], [45]:

Heterogeneity: Fog Computing leverages virtualization to provide a versatile platform. This enables it to offer diverse computing, storage, and networking services tailored to the requirements of various applications and devices. Heterogeneity allows fog computing to bridge the gap between resource-constrained IoT devices and the robust infrastructure found in traditional Cloud Data Centers[46]-[48].

Edge Location: Fog Computing's emphasis on edge locations brings services closer to the end-users or devices. This proximity significantly reduces latency, ensuring a seamless user experience for applications like gaming, video streaming, and augmented reality. Fog Computing optimizes bandwidth usage and decreases the load on centralized data centers. Edge location is particularly crucial in scenarios where network bandwidth [49]-[51] is limited or where real-time decision-making is required, such as autonomous vehicles, VANETS or industrial automation. [52], [53].

Geographical Distribution: Fog Computing's geographical distribution is in stark contrast to the centralized nature of traditional Cloud Computing. It focuses on distributing services widely across different locations and regions. This approach enhances the resilience and redundancy of services, as they can continue to operate even if certain locations are affected by disruptions or failures [54]-[56].

Large-Scale Sensor Networks: Fog Computing plays a critical role in managing large-scale sensor networks used in applications like environmental monitoring and Smart Grids [57]-[61]. These sensor networks generate vast amounts of data that require distributed computing and storage resources for processing and analysis.

Extensive node count: Fog Computing's extensive geographical distribution often leads to a large number of interconnected nodes, such as edge devices, gateways, and Fog Nodes. This multitude of nodes contributes to the overall scalability of the Fog Computing architecture, allowing it to adapt to various workloads and traffic patterns. It also necessitates effective management and monitoring tools to ensure the smooth operation of the distributed system. [58]-[66].

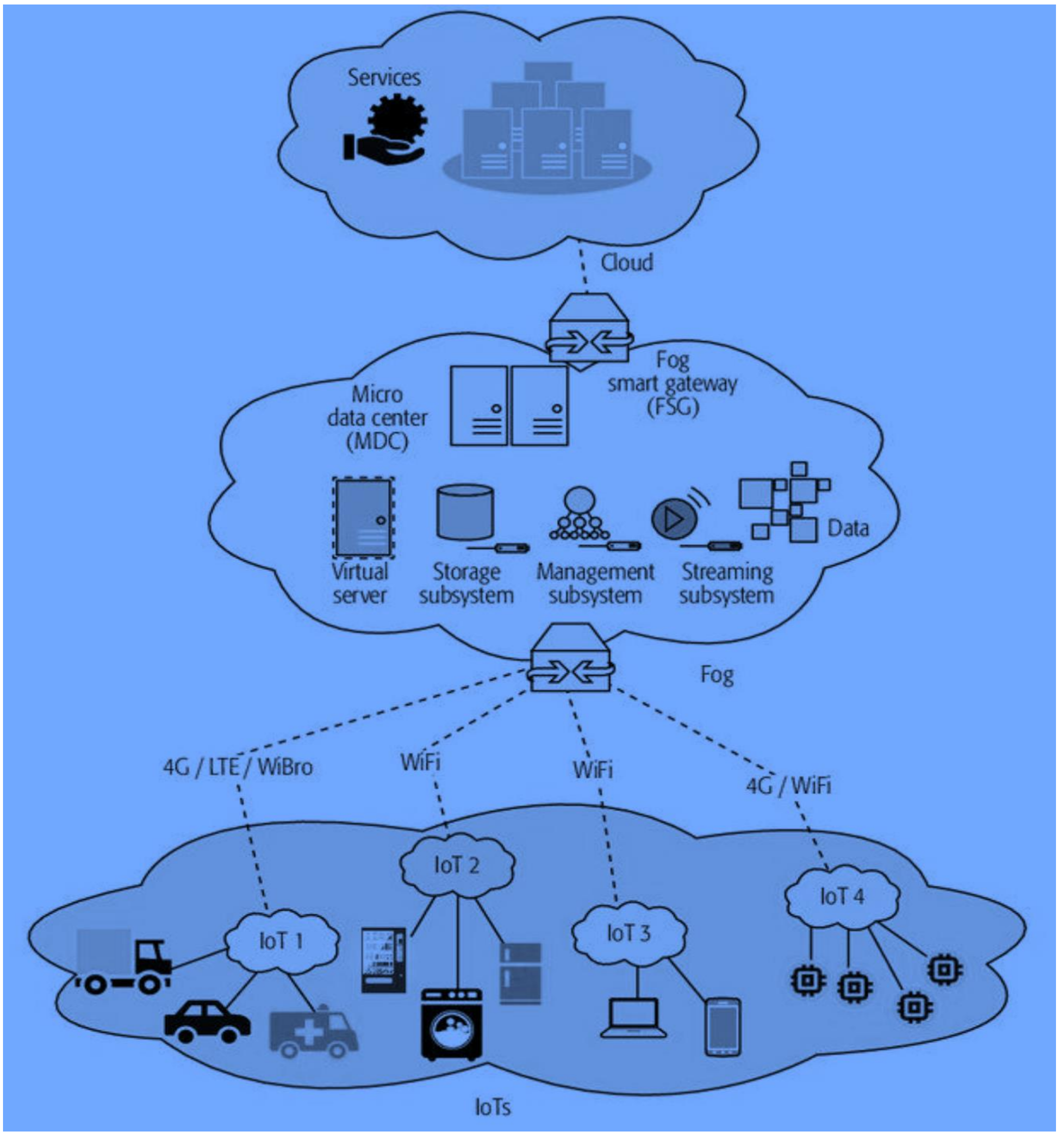

Figure 2 The Fog Components and Integration

Mobility Support: Many Fog Computing applications involve direct communication with mobile devices, which may change their location frequently. To support this mobility, Fog Computing incorporates techniques such as the Locator/ID Separation Protocol (LISP). LISP decouples the identity of a host from its location, ensuring that the host can move between different network segments without changing its IP address and where a distributed directory system is employed to maintain up-to-date mappings between host identities and their current locations [67]-[71].

Real-Time Interactions: Fog Computing is well-suited for applications that require real-time interactions and rapid decision-making. These applications include autonomous vehicles that rely on immediate sensor data analysis, industrial automation systems that need low-latency control, and augmented reality applications that demand responsive user experiences [72], [73].

2.4. Related Work

Over the last years, many scholars have extensively explored the privacy and security concerns within the domain of Fog computing, predominantly providing a broad overview of these privacy and security issues. To underscore the significance of the subject matter addressed in our article, "Privacy and Security Issues in Fog-to-Fog Communication," this section focuses on a thorough examination of prior research conducted in the field of fog computing. In the **Table 1** below, we present a survey of research papers, outlining their key objectives, key lessons learned and valuable contributions published from 2020 to 2023.

Table 1 Comparative Analysis of Review Papers.

Ref.	Year	Aims and Objectives	Lesson Learned	Key Contribution
[74]	2023	The objective of this article is to comprehensively address the risks, challenges, and potential solutions associated with security in fog computing. It also sheds light on ongoing research within the realm of fog computing.	Overview of threats in fog computing paradigm, and that threats remains a big demand for security and confidentiality measures.	The paper outlines the risks, issues and solutions that are linked to security in fog computing. It then includes information on ongoing research projects, covering security and safety concerns in fog computing paradigm.
[75]	2023	The main objective of this paper is to address the technical challenges and research gaps in fog computing. It offers a comprehensive perspective and aims underscores the significance of security and privacy issues prioritization in fog computing.	Fog Computing has capabilities of making good decisions and trying better service in the future with the help of various protocols used to maintain IoT.	The article summarizes the latest advances and developments in the realm of fog computing. It offers insights on the solutions to security and privacy issues, more particularly to data management issues associated with fog computing.
[76]	2023	The paper gives in-depth insights on possible hazards within interconnected systems. The article expounds security threats, vulnerabilities and privacy concerns.	Fog or Cloud Based IoT Systems [77] security measures must be strengthened to keep up with the ever-evolving cybersecurity landscape.	The paper highlights the extensive demand for comprehensive privacy and security to support Fog and Cloud Computing.
[78]	2023	The paper discusses cloud computing with particular emphasis on the paradigms that preceded the fog computing emergence. It also identifies the key challenges associated with fog computing to provide information to researchers in this evolving field.	The research highlights the prominence of security, privacy, application, and communication challenges within the contributions made by scholars in the field.	The paper discusses cloud computing, proposed taxonomy and furnishes an in-depth analysis of how security, privacy, application, and communication challenges feature in the scholarly contributions.
[79]	2022	This paper presents a list of security and privacy in fog computing paradigm. It also expounds dangers that exist in cloud, fog and edge computing paradigms.	Fog computing is prone to various numerous security and privacy concerns.	The article discusses the privacy and security issues in fog computing ecosystem. The article also highlights the existing dangers in cloud, fog and edge computing.
[80]	2022	The objective of this article is to give the state-of-the-art in fog computing architectures, security	Fog computing security challenges and the	The paper gives insights on the security challenges countermeasures in fog

		challenges and the existing countermeasures to guide researchers to find comprehensive information and solutions in fog computing.	corresponding countermeasures.	computing, hence helping researchers with solutions in fog computing systems.
[81]	2022	The main objective of this paper is to discuss the implementation of fog computing and proposing efficient approach for encryption to strengthen security on fog computing.	Efficient encryption approach for providing security in fog computing.	The article suggests an effective encryption method to enhance security within the domain of fog computing.
[41]	2021	The objective of this article is to provide a comprehensive analysis of the privacy and security challenges associated with fog computing.	Fog computing paradigm confidentiality and security issues	The article discusses the confidentiality concerns and issues in fog computing; and suggests methods for mitigating these difficulties in fog computing.
[82]	2021	The primary objective of this article is to offer an extensive exploration of the privacy and security concerns associated with Fog computing. The paper aims to do a thorough survey of the existing literature on Fog computing, aiming in synthesizing the current state-of-the-art knowledge regarding the security and privacy challenges.	Fog computing categories; network services and communications, Data processing (inside Fog node), and IoT device's privacy (end-user device)	The paper recognizes that the conventional privacy and security solutions tailored for Cloud computing cannot be directly transplanted to the Fog computing domain due to its unique characteristics. The paper also underscores the essential need for context-specific solutions to address security and privacy challenges in the Fog environment.
[83]	2021	The paper organized recent studies and examined fog computing, identified challenges related to their design and highlighted arears for further research and future opportunities.	Fog computing progress will lead to additional paradigms to enhance service delivery.	The paper addressed fog computing research status, highlighted areas of further research, and future opportunities.
[84]	2021	The paper identifies and discusses the security challenges in fog computing. It also gives insights on blockchain approach to mitigate the security concerns.	Blockchain technology [85] can be used to mitigate the privacy and security concerns in fog computing.	The paper discusses the security and privacy challenges in fog computing. The paper provides overview on how Blockchain can mitigate most of these challenges.
[86]	2021	The article explores the security access control technology within the context of fog computing. It examines its essential components and a detailed analysis of two key dimensions: extended access and hidden access. It aims to provide users with a broader range of flexible access control options in fog computing environments	Ensuring the security of user data in fog computing environments necessitates robust collaboration and communication among various functional modules.	The research examines security access control technology in fog computing, hence efficient and effective protection mechanism of data security.
[87]	2021	The article conducts a comprehensive examination of the challenges and concerns faced by Fog computing, with a specific focus on privacy and security issues.	The paper highlights the challenges encountered within the landscape of security and privacy issues in fog computing and IoT.	The significant contribution of this paper lies in the introduction of an area privacy protection algorithm that safeguards location privacy hence maintaining low

				computational and communication overhead.
[88]	2021	The paper explains blockchain, its architecture, and its security. It further explains how Blockchain application is applied in IoT security including fog computing and generic Security requirements for fog computing.	The paper discusses how blockchain application is applied in fog computing to enhance security.	This paper emphasizes the important role of the blockchain technology in strengthening security in IoT and fog computing. The paper also gives insights on improving security in IoT and fog computing.
[89]	2021	The paper conducts a comparative study of existing fog architectures then perform a critical analysis of different authentication schemes in Fog computing. It also highlights some key strategies of enhancing the IoT devices.	The adoption of computational centric architectures, more secured payment systems can help in designing and deploying distributed, decentralized systems	This paper's key contribution lies in its affirmation that the absence of a standardized architecture for Fog computing, particularly in trust management and privacy that lead to potential security threats to the IoT.
[90]	2020	The study explores fog computing, highlighting its concerns and challenges. The paper also introduces future research areas discussed.	Fog computing plays a critical in making IoT technologies and networks work efficiently.	The study provided a summary of fog computing, highlighting its challenges and key points, as it gives future research direction.
[91]	2020	The study offers a thorough examination of fog and edge computing, aiming to create a foundation for solutions in the domain of Internet of Things, Fog computing and cloud environments.	The use of advanced technologies such as the Machine Learning (ML) and Artificial Intelligence (AI) help enhance fog computing.	The article laid the groundwork for solutions in research related to Internet of Things, Fog computing and cloud environments. It explored the tools for these environment setups.
This Paper	2023	The paper explores privacy and security concerns in fog-to-fog (F2F) communication within the fog computing framework. It offers comprehensive understanding of complex landscape of privacy and security in fog-to-fog communication.	The privacy and security issues in Fog-to-Fog (F2F) Communication.	This paper extensively explores privacy and security issues in fog-to-fog (F2F) communication within the fog computing framework. It provides a thorough background on fog computing, discusses current concerns in F2F communication, and identifies research gaps.

3. Research Methodology

In this survey paper, we analyse existing literature on privacy and security issues in fog-to-fog (F2F) communication. The research methodology involved a comprehensive review of academic papers, conference proceedings, and relevant publications. The rigorous selection process aimed to provide a holistic and up-to-date overview of the current state of research in this field. Available research work for the last three years (2020 - 2023) where examined to identify the relevant literature. The methodology employed to establish privacy and security issues in Fog-to-Fog Communication (F2F) comprised three distinct steps:

3.1. String Searching

On 7th November, 2023, a search string was conducted using the Boolean Operators effectively retrieve the literature that is related to the study. The keywords included in the search string include “Fog-to-Fog Communication”, “F2F” “Fog Computing”, “Privacy”, “Security”, “F2F-IoT”. Boolean operators such as “OR”, “AND” were utilized to enhance the search through advanced search. To broaden the search scope by retrieving the articles containing any of the specified keywords, "OR" Boolean operator was employed. "AND" operator was then employed to narrow down the search and obtain the articles that included the specified keywords. These Boolean operators ensured more focused and specified selection of the literature. This string search approach gave room for more comprehensive and systematic literature exploration related to privacy and security issues in Fog-to-Fog (F2F) Communication. Figure3 explains the search process.

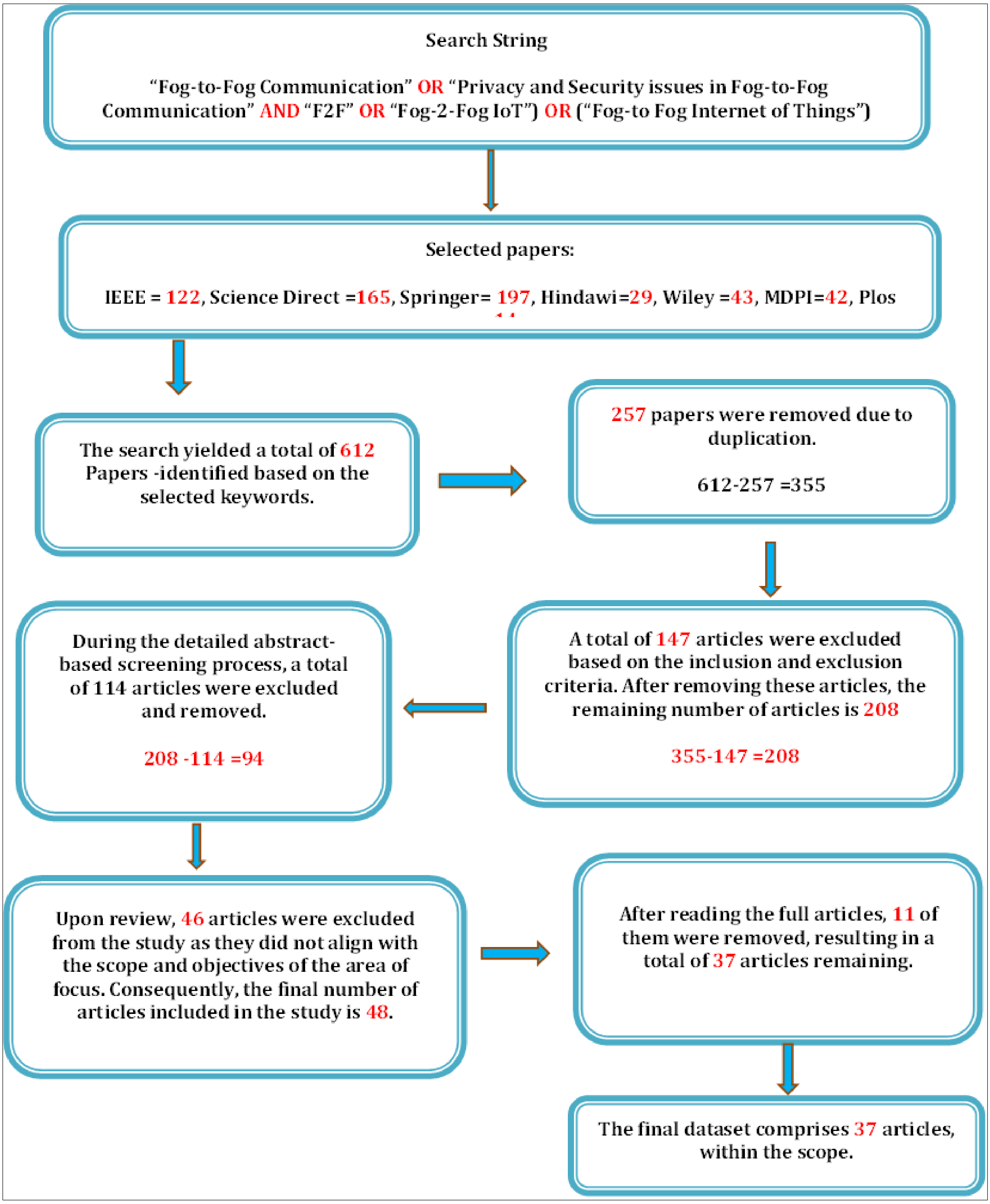

Figure 3 The selection and screening process

3.2. Data Sources

In this study, the data sources encompassed selection of articles from the most renowned academic databases, namely, the IEEE, ScienceDirect, Springer, Hindawi, Wiley, MDPI and Plos. The academic databases were chosen because of their extensive collection of excellent scholarly articles relevant to the area of study. Table 2 shows the selected databases and the number of scholarly articles after the string search.

Table 2 Selected Databases

Database Name	Database URL	Number of Articles
IEEE	https://ieeexplore.ieee.org/	122
ScienceDirect	https://www.sciencedirect.com	165
Springer	https://www.springer.com	197
Hindawi	https://www.hindawi.com	29
MDPI	https://www.mdpi.com/	42
Plos	https://plos.org	14
Wiley	https://onlinelibrary.wiley.com/	43

3.3. Screening of the papers

The screening process was applied to the articles identified during the string search process as explained above. The first step involved assessments based on the abstract content, the keywords and the titles to examine their relevance with the area of study. The papers that met the predefined search criteria where then subjected to more detailed review to determine their alignment with privacy and security issues in fog-to-fog communication. In the process, articles that provided significant insights into the privacy and security issues in fog-to-fog communication were analyzed further, and the papers that did not align with the scope and objective of the study were excluded. This in-depth screening of papers process ensured that relevant articles were included in the study hence contributing immensely to the robustness of the research study.

4. Analysis of the Reviewed Literature

This section offers a thorough examination of the findings derived from the reviewed survey papers. Fog computing has received substantial attention from researchers, resulting in a diverse array of perspectives and topics. Scholars have made significant contributions to fog computing, particularly in the domains of privacy, security, data management, and communication. In this paper, we undertake an in-depth analysis of the current state of security and privacy issues in Fog-to-Fog (F2F) within the realm of fog computing. Researchers have demonstrated a strong emphasis on fog computing, and this survey, in particular, delves extensively into the specific aspects of privacy and security in Fog-to-Fog Communication. **Table 1** provides clear examination of existing literature, and comparative analysis with the paper.

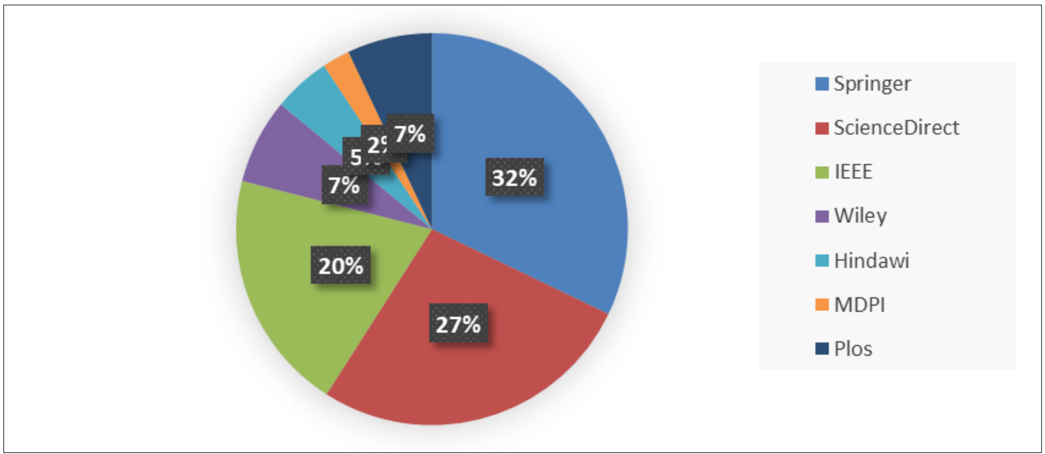

Figure 4 Article Selection Analysis.

4.1. Privacy and Security Issues in F2F Communication

Following the extensive review, the study identified several research gaps in privacy and security concerns in within the domain of fog-to-fog communication. Many researchers have focused so much on Fog Computing. According to [92],many applications in fog computing are primarily driven by the desire for efficient services and user satisfaction, often overlooking the importance of security requirements or treating them as secondary considerations. The privacy and security concerns in fog computing have not received adequate attention [93], leading to potential vulnerabilities and risks within this emerging technology. The insufficient focus on security aspects in fog computing may expose systems and data to various threats, including unauthorized access, data breaches, and other cyber threats [94], [95].

Many experts are working to find answers for different aspects of fog computing. But, the problem of privacy and security in fog-to-fog communication is still a big challenge in both academic and industrial setting [96]. As indicated in [97], fog computing presents several challenges in terms of security and privacy. These challenges encompass restricted network visibility, inadequacies in detecting attacks, the lack of user-selective data collection, virtualization issues, challenges related to multitenancy, and issues arising from malicious fog nodes. It is crucial to effectively handle mutual authentication, secure key exchange, and anonymity to ensure sufficient security and privacy in the tiers of fog computing [92]. Access control stands out as a widely employed preventive strategy, aiming to safeguard against unauthorized access and mitigate the impact of security breaches in fog ecosystem [98].

4.2. Trust issues in Fog-to-Fog Communication

Establishing and maintaining trust in fog computing is very crucial in ensuring data integrity, availability and confidentiality. Authors in [99] defines trust as a two-way process between fog node and a device to ensure robust security between them. Secure communication forms the bedrock of a trusted relationship among devices as highlighted in [100], [101].The most common trust issues in fog computing are summarized in Table 3.

- Trust in Node Authentication: Trust in Node Authentication addresses the challenge of verifying the authenticity of fog nodes. Effective authentication is important in establishing trust in IoT devices [102], [103].
- Trust in Data Integrity: Trust in data integrity revolves around the ability to trust that data remains unmodified or untampered during the data transmission. The privacy-preserving techniques help in enhancing trust [104], [105], [102].
- Trust in access control: Trust in access control is paramount in ensuring that only authorized fog nodes communicate with each other. If trust in access control is compromised, then data and communication will be prone to unauthorized access [105], [102].
- Trust in Encryption: Trust in Encryption emphasizes on the importance of trusting the encryption methods for the data in transit [100].
- Trust in Identity Management: This involve trusting the accuracy and reliability of fog node identities in fog communication [106].
- Trust in Redundancy and failover mechanisms: Trust in Redundancy and failover mechanisms focuses on the reliability of mechanisms that maintain service availability [107]-[109]. A robust trust evaluation model is proposed in [110].

4.3. Authentication and Authorization

Fog nodes must be able to authenticate each other to ensure that communication is only established between trusted entities. [122] defines authentication as to identify every connected fog node as a verified node. It further defines authorization as to describe the privileges of each connected node. Authentication in fog nodes can be used to reduce latency [123].

Authentication is very important as weak authentication mechanisms can lead to unauthorized access and potential security breaches [102]. Unauthorized fog nodes attempting to communicate with each other could compromise the overall security of the fog computing environment. Effective access control mechanisms are essential to prevent unauthorized access. Only the authorized users can have access to the specified network resources. They are implemented to strengthen trust [104], [105], hence enhance enhancing privacy and security in fog ecosystem.

5. Data Privacy

As data is transmitted between fog nodes, there is a risk of interception. Without proper encryption mechanisms, attackers could eavesdrop on the communication, leading to unauthorized access to sensitive information. Fog nodes are required to share data with the devices they want to share their data [124]. To make sure the privacy of users in fog-to-fog communication, it's important to figure out ways to recognize obfuscation [125]. Obfuscation means intentionally making information unclear or hard to understand. In fog computing and IoT, this might involve hiding sensitive details to protect user privacy. This strengthens confidentiality of the user information in transit.

Recognizing obfuscation is like being proactive to protect the privacy of IoT users. It helps fog computing systems tell the difference between efforts to keep sensitive data safe and actions that might try to misuse or harm user privacy [126], [127]. This is crucial for finding the right balance between keeping data safe and making sure the system works as intended. Creating strong methods to spot and handle obfuscation is in line with the main aim of respecting user privacy in fog computing. It ensures that privacy measures work well without getting in the way of how IoT systems are supposed to function.

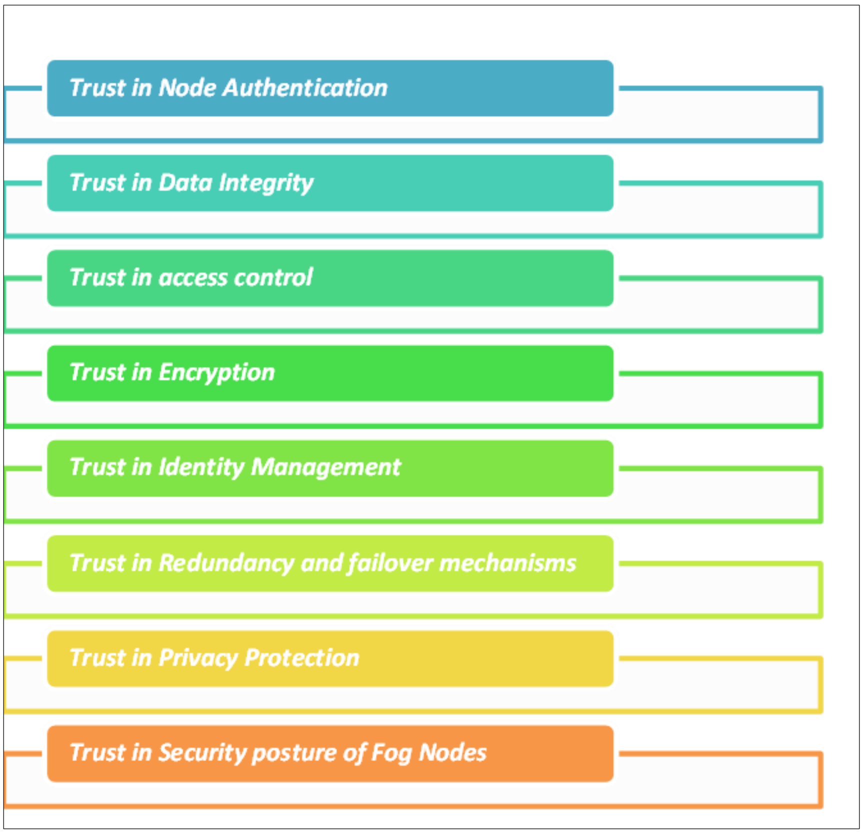

Figure 5 Graphical Overview of Trust issues in Fog-to-Fog Communication

Trust in Privacy Protection: Users must trust that their data is handled in privacy and secured manner, erosion of trust can lead to concerns about privacy and security violations [11],[110].

Trust in Security posture of Fog Nodes: This highlights the necessity to trust the privacy and security measures that are implemented on individual fog nodes.

Table 3 Summary of Trust Issues in Fog Computing

S/No	Trust Criteria	Issue	Explanation
1	Trust in Node Authentication	Lack of trust in the authenticity of communicating fog nodes.	Effective authentication mechanisms are essential for establishing trust between fog nodes. If nodes cannot reliably authenticate each other, the entire communication system's security is compromised [112].
2	Trust in Data Integrity	Inability to trust that data has not been tampered with during transmission.	Ensuring the integrity of data requires trust in the mechanisms in place to detect and prevent tampering [113]. Without this trust, the data's reliability is undermined.

3	Trust in Access Control	Insufficient trust in the access control mechanisms governing fog-to-fog communication.	Trust in access controls is necessary to ensure that only authorized fog nodes can communicate with each other [114]. If this trust is compromised, unauthorized access may occur.
4	Trust in Encryption	Lack of trust in the encryption methods used to secure data in transit.	Encryption is a fundamental component of securing communication [115]. Trust in the encryption algorithms and key management practices is essential to guarantee the confidentiality of the data being transmitted.
5	Trust in Identity Management	Lack of trust in the accuracy and reliability of fog node identities.	Trust in the identity management system is crucial to prevent identity spoofing and unauthorized access [116], [117]. If identity information is compromised, trust in the entire communication system is at risk.
6	Trust in Redundancy and failover mechanisms	Inability to trust the reliability of redundancy and failover mechanisms.	Redundancy and failover mechanisms are critical for maintaining service availability [118], [119]. If these mechanisms are not trustworthy, the system may fail to recover from disruptions, impacting the overall trustworthiness of the communication infrastructure.
7	Trust in Privacy Protection	Lack of trust in the privacy measures implemented to protect user data.	Users must trust that their data is handled in a privacy-preserving manner [120]. If this trust is eroded, it can lead to concerns about data misuse and privacy violations.
8	Trust in Security posture of Fog Nodes	Inability to trust the security measures implemented on individual fog nodes.	Each fog node contributes to the overall security of the communication system. If there is a lack of trust in the security posture of individual nodes, the entire system's security is compromised [121].

5.1. Integrity of Communication

Ensuring the integrity of communication in fog-to-fog settings means making sure that the information shared between different fog nodes doesn't get messed with or changed during the exchange [128]- [132]. It's like keeping a promise that the data stays accurate and reliable. To tackle this, we use clever tools like encryption, which is like a secret code that only the right fog nodes can understand. We also check for any unusual changes in the communication patterns and have ways to confirm that the messages are genuine and haven't been tampered with. It's a bit like sending a letter in a locked box with a special key that only the intended recipient has, making sure nobody messes with the contents along the way. All these measures are essential to build trust and keep the information safe as it moves between fog nodes in a fog computing system.

5.2. Resource Constraints

Fog nodes often have resource constraints, including limited processing power and memory [133], [134]. This can make it challenging to implement robust security measures, and attackers may exploit these limitations to compromise the security of fog-to-fog communication.

5.3. Denial of Service (DoS) Attack

Malicious actors might intentionally overwhelm or flood the communication channels between fog nodes, disrupting normal operations. It's akin to a traffic jam on the information highway, preventing legitimate data from flowing smoothly [135]. This not only impacts the availability and reliability of services but also creates a vulnerability where sensitive information might be exposed due to the communication breakdown.

5.4. Dependency on Network Infrastructure

Fog computing relies on network connectivity, and disruptions in the network can impact communication between fog nodes. Redundancy and failover mechanisms need to be in place to address these concerns. Implementations of systems like Intrusion Prevention Systems (IPS) in fog computing have strengthened trust [136].

Table 4 below provides a structured overview of the privacy and security concerns in fog-to-fog communication, detailing the domain, sub-domain, issue, and an explanation for each concern.

Table 4 Structured overview of privacy and security issues

S. No	Privacy and Security Domain	Privacy and Security Sub-Domain	Privacy and security Issue	Explanation
1	Data Privacy	Data Transmission	Data Interception	Unencrypted data transmission between fog nodes can be intercepted by malicious actors, leading to unauthorized access [137] and many potential data breaches.
2	Data Integrity	Data Transmission	Data Tempering	Unauthorized modification of data during transmission between fog nodes can compromise its integrity, affecting the authenticity and trustworthiness of the communicated data [138].
3	Identity Management	Authentication	Insufficient Authentication	Unauthorized modification of data during transmission between fog nodes can compromise its integrity, affecting the authenticity and trustworthiness of the communicated data.
4	Identity Management	Authentication	Identity Spoofing	Insufficient identity verification mechanisms may allow malicious nodes to impersonate legitimate fog nodes, leading to unauthorized access and potential manipulation of communication [139].
5	Access Control	Authorization	Access Control Vulnerabilities	Inadequate access controls may allow unauthorized fog nodes to gain access to sensitive data or services, posing a significant security risk [140], [141].
6	Data Privacy	Data Transmission	Data Leakage	In the absence of proper data protection measures, unauthorized exposure of sensitive information during communication can lead to privacy violations and legal consequences [142].
7	Resource Management	DoS Attacks	Resource Exhaustion Attacks	Overloading fog nodes with excessive communication requests can lead to denial of service [143], impacting the availability of services and disrupting normal operations.
8	Configuration Management	Fog Node Configuration	Insecure Fog Node Configuration	Poorly configured fog nodes introduce vulnerabilities [144], enabling attackers to exploit weaknesses and compromise the overall security of fog-to-fog communication.
9	Encryption Management	Key Management	Lack of Encryption Key Management	Inadequate management of encryption keys can result in unauthorized access to encrypted data [145], undermining the confidentiality of fog-to-fog communication.
10	Interoperability	Standardization	Interoperability Challenges	Lack of standardized protocols and inconsistent implementations can introduce interoperability issues [146], potentially leading to security vulnerabilities in fog-to-fog communication.

11	Privacy	Metadata	Privacy violations through metadata	Inadvertent exposure of sensitive information through metadata can lead to privacy violations, even if the actual content is encrypted[147], [148].
12	Forensic Analysis	Forensic Capabilities	Limited Forensic capabilities	The distributed and resource-constrained nature of fog nodes may limit the ability to conduct thorough forensic analysis, hindering the identification and mitigation of security incidents [149].
13	Network Dependency	Network Connectivity	Dependency on external networks	Fog computing's dependence on external networks introduces risks related to network stability and connectivity [150], impacting the reliability and security of fog-to-fog communication
14	Update Management	Security updates	Inadequate update mechanisms	The lack of a robust mechanism for applying security updates may allow vulnerabilities in fog node software to persist [151], exposing the communication to potential exploitation.

5.5. Countermeasures in Fog-To-Fog Communication

5.5.1. Data Privacy and Transmission Security

To safeguard data during transmission, it's crucial to use end-to-end encryption. This means the data is protected throughout its journey between fog nodes. Implementing secure communication protocols like TLS/SSL and strong authentication mechanisms ensures that only authorized fog nodes can access and exchange data securely [152], [153].

5.5.2. Data Integrity

To maintain data integrity, cryptographic techniques such as digital signatures play a key role. They act like virtual fingerprints, assuring that the data hasn't been altered during its journey. Implementing checksums or hash functions provides a quick way to detect any unauthorized changes, allowing for timely responses [154].

5.5.3. Identity Management and Authentication

Strong identity management and authentication methods are crucial. Fog nodes need to reliably verify each other's identities before engaging in communication. This involves secure key exchange protocols and, for an extra layer of security, the integration of biometric or multi-factor authentication methods [155]-[159]. With the help of user credentials like passwords, authentication is achieved.

5.5.4. Access Control and Authorization

Robust access controls ensure that only authorized fog nodes can access sensitive data or services. Role-based access control (RBAC) structures limit access based on user roles, and regular reviews and updates of access control policies help maintain a secure environment [160], [161]. Network segmentation adds an extra layer of protection. Access control is essential in preserving privacy and security in fog-to-fog communication.

5.5.5. Resource Management and Denial of Service (DoS) Protection

To protect against resource exhaustion attacks and ensure the availability of services, implementing rate limiting, traffic filtering, load balancing, and detection and response mechanisms for denial of service (DoS) attacks are essential countermeasures [162].

5.5.6. Configuration Management

Security vulnerabilities often stem from poorly configured fog nodes [163]. Implementing security best practices, conducting regular security audits, and employing automated tools for configuration management and security compliance help maintain a secure configuration.

5.5.7. Encryption Key Management

Proper encryption key management involves establishing a robust system [164]. This includes secure key generation, storage, and distribution. Regularly rotating encryption keys and using hardware security modules (HSMs) enhance the overall security of fog-to-fog communication.

5.5.8. Interoperability Challenges

Overcoming interoperability challenges requires adherence to standardized communication protocols [165], [166]. Active participation in standardization efforts fosters compatibility, and implementing middleware solutions facilitates seamless communication across diverse fog computing environments.

5.5.9. Privacy Concerns through Metadata

Safeguarding against privacy violations through metadata involves minimizing the collection and storage of unnecessary metadata [167]-[171]. Techniques like data anonymization or pseudonymization add an extra layer of protection. Regular reviews and updates of privacy policies ensure alignment with evolving privacy standards.

5.5.10. Limited Forensic Capabilities

The challenge of limited forensic capabilities necessitates adaptive strategies [172]. Implementing logging mechanisms for relevant security events, integrating security information and event management (SIEM) solutions, and considering the use of distributed forensic tools ensure comprehensive investigative capabilities.

5.5.11. Inadequate Update Mechanisms

Addressing the vulnerability stemming from inadequate update mechanisms demands a systematic approach [174]. Establishing a proactive process for timely application of security updates, leveraging automated patch management tools, and conducting regular vulnerability assessments are indispensable for maintaining a secure fog computing environment.

5.5.12. Dependency on External Networks

Mitigating risks associated with dependency on external networks requires a resilient strategy [175-[177]. Implementing redundancy and failover mechanisms ensure operational continuity during network disruptions. Exploring edge computing solutions that function autonomously during intermittent connectivity further enhances the reliability and security of fog-to-fog communication. Implementations of systems like Intrusion Detection Systems (IDS) in fog computing enhance security threat elimination [179].

Table 5 provides a quick reference on the key countermeasures to address privacy and security concerns in fog-to-fog communication.

Table 5 Summary of the key countermeasures

S/No	Domain Area	Countermeasure
1	Data Privacy and Transmission Security	Implement end-to-end encryption (e.g., TLS/SSL). Use secure communication protocols [179]. Enforce strong authentication.
2	Data Integrity	Apply cryptographic techniques (e.g., digital signatures) Implement checksums or hash functions for unauthorized changes [180].
3	Identity Management and Authentication	Deploy strong mutual authentication methods Utilize secure key exchange protocols Integrate biometric or multi-factor authentication [181]-[183]
4	Access control and Authorization	Implement role-based access control (RBAC) [184] Regularly review and update access control policies. Use network segmentation.

5	Resource Management and DoS protection	Implement rate limiting and traffic filtering. Use load balancing. Deploy detection and response mechanisms for DoS attacks [185].
6	Configuration Management	Follow security best practices for configuring fog nodes. Conduct regular security audits. Use automated tools for configuration management [186]
7	Encryption Key Management	Establish a robust key management system [187]-[189] Regularly rotate encryption keys Use hardware security modules (HSMs)
8	Interoperability Challenges	Adhere to standardized communication protocols Participate in standardization efforts Implement middleware solutions for compatibility [190].
9	Privacy concerns through metadata	Minimize collection of unnecessary metadata Implement data anonymization or pseudonymization [191]-[194]. Regularly review and update privacy policies
10	Limited Forensic Capabilities	Implement logging mechanisms for security events Integrate SIEM solutions for centralized log analysis [195] Consider distributed forensic tools
11	Inadequate update mechanisms	Establish a systematic process for applying security updates Use automated patch management tools Conduct regular vulnerability assessments [196].
12	Dependency on external networks	Implement redundancy and failover mechanisms [197] Explore edge computing solutions for autonomous functionality during connectivity issues

5.6. Open Research Gaps and Future Directions

The present research gaps in Fog-to-Fog Communication lie at the intersection of the rapid technological advancements and the implementation challenges. Fog computing has presented a promising paradigm for decentralized computing, gaps persist in optimizing resource allocation and workload distribution in the dynamic fog ecosystem.

There's need for standardized protocols and robust frameworks to bolster the interoperability among the heterogeneous fog nodes. If fog devices are linked to the system, they could potentially initiate attacks triggered by alterations in signals or movements within the cloud environment. The privacy preserving techniques, especially data-intensive applications, require further exploration to strike an equilibrium between efficient data processing and protecting sensitive information.

The future of fog-to-fog communications will lead to address the several ever evolving challenges and capitalize on emerging opportunities. The key avenue involves advancing the protocols, machine learning and artificial intelligence algorithms tailored for fog ecosystem hence enabling more advanced and intelligent decision making at the edge. Scholars and practitioners should also focus on developing more dynamic and adaptive resource management strategies.

This will optimize the allocation of the computational resources within fog network. Integration of blockchain technology to bolster security, transparency and trust in fog ecosystem is also an area ripe for exploration. Energy efficient communication protocols, resilient fault tolerant mechanisms and sustainable fog infrastructure are also very important for long term viability of fog-to-fog communication.

6. Conclusion

Privacy and security issues in fog-to-fog communication underscores the critical importance for comprehensive strategies to safeguard and protect sensitive information in a decentralized computing environment. The identified issues, ranging from various forms of trust, authentication, authorization, access control, DoS attacks, dependency on external networks, emphasize on the multifaceted nature of privacy and security issues in fog-to-fog communication. Implementing robust countermeasures as outlined in this discussion is essential in mitigating these issues. It's very crucial to address the privacy and security concerns in the ever-evolving digital era of fog computing. This concerns when fully addressed will be fundamental in building trust and realizing the full potential of fog-to-fog communication in diverse industry domains.

Compliance with ethical standards

Acknowledgements

The author expresses deep gratitude to his esteemed professors and academic mentors at Jaramogi Oginga Odinga University of Science and Technology (JOOUST). Special thanks to Dr. Vincent Nyangaresi, Prof. Anthony J . Rodrigues, Prof. Solomon Ogara, Dr. Joshua Agola, Prof. Samuel Liyala, Dr. Richard Omolo, Dr. Leonard Wakoli, Dr. Castro Yoga, Dr. Samuel Olala, and all the dedicated academic and non-academic staff of the Department of Computer Science and Software Engineering, School of Informatics and Innovative Systems.

Additionally, sincere appreciation is extended to the entire team in IT Security and Audit, including Mr. Felix Oroo, Miss. Janet Angud'i, Mr. Collins Omondi, Mr. Jeremiah Okeyo, and Mr. Emmanuel Asituha, for their valuable contributions and support.

Disclosure of conflict of interest

The authors declares that there are no competing interests.

References

[1] Baker SA, Rashid SJ. Fog Computing: A Comprehensive Review of Architectures, Applications, and Security Challenges. NTU Journal of Engineering and Technology. 2023 Oct 17;2(2).

[2] Burhan M, Alam H, Arsalan A, Rehman RA, Anwar M, Faheem M, Ashraf MW. A comprehensive survey on the cooperation of fog computing paradigm-based iot applications: layered architecture, real-time security issues, and solutions. IEEE Access. 2023 Jul 12.

[3] Zhao J, Zeng P, Choo KK. An efficient access control scheme with outsourcing and attribute revocation for fog-enabled E-health. IEEE Access. 2021 Jan 18;9:13789-99.

[4] Wu TY, Lee Z, Obaidat MS, Kumari S, Kumar S, Chen CM. An authenticated key exchange protocol for multi-server architecture in 5G networks. IEEE Access. 2020 Jan 28;8:28096-108.

[5] Nabeeh NA, Abdel-Basset M, El-Ghareeb HA, Aboelfetouh A. Neutrosophic multi-criteria decision making approach for iot-based enterprises. IEEE Access. 2019 Apr 2;7:59559-74.

[6] Yu R, Xue G, Kilari VT, Zhang X. The fog of things paradigm: Road toward on-demand Internet of Things. IEEE Communications Magazine. 2018 Sep 16;56(9):48-54.

[7] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22;6(7):154.

[8] Iqbal R, Butt TA, Afzaal M, Salah K. Trust management in social internet of vehicles: factors, challenges, blockchain, and fog solutions. International Journal of Distributed Sensor Networks. 2019 Jan;15(1):1550147719825820.

[9] Yassine A, Singh S, Hossain MS, Muhammad G. IoT big data analytics for smart homes with fog and cloud computing. Future Generation Computer Systems. 2019 Feb 1;91:563-73.

[10] Alzoubi YI, Osmanaj VH, Jaradat A, Al-Ahmad A. Fog computing security and privacy for the Internet of Thing applications: State-of-the-art. Security and Privacy. 2021 Mar;4(2):e145.

[11] Tariq N, Asim M, Al-Obeidat F, Zubair Farooqi M, Baker T, Hammoudeh M, Ghafir I. The security of big data in fog-enabled IoT applications including blockchain: A survey. Sensors. 2019 Apr 14;19(8):1788.

[12] Khan S, Parkinson S, Qin Y. Fog computing security: a review of current applications and security solutions. Journal of Cloud Computing. 2017 Dec;6(1):1-22.

[13] Nyangaresi VO, Abood EW, Abduljabbar ZA, Al Sibahe MA. Energy Efficient WSN Sink-Cloud Server Authentication Protocol. In2021 5th International Conference on Information Systems and Computer Networks (ISCON) 2021 Oct 22 (pp. 1-6).

[14] Kumar D, Rishu, Annam S. Fog Computing Applications with Decentralized Computing Infrastructure—Systematic Review. InProceedings of the Seventh International Conference on Mathematics and Computing: ICMC 2021 2022 Mar 6 (pp. 499-509). Singapore: Springer Singapore.

[15] Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications. 2022 Jun 21.

[16] Shinde SV, Hemanth DJ, Elhoseny M. Introduction to different computing paradigms: cloud computing, fog computing, and edge computing. InIntelligent Edge Computing for Cyber Physical Applications 2023 Jan 1 (pp. 1-16). Academic Press.

[17] Rajkumar K, Hariharan U. Moving to the cloud, fog, and edge computing paradigms: Convergences and future research direction. InArtificial Intelligence and Machine Learning for EDGE Computing 2022 Jan 1 (pp. 425-442). Academic Press.

[18] Verma U, Bhardwaj D. Fog Computing Paradigm for Internet of Things Applications. Ambient Intelligence and Internet of Things: Convergent Technologies. 2022 Dec 20:243-71.

[19] Krishnaraj N, Daniel A, Saini K, Bellam K. EDGE/FOG computing paradigm: Concept, platforms and toolchains. InAdvances in Computers 2022 Jan 1 (Vol. 127, pp. 413-436). Elsevier.

[20] Abduljabbar ZA, Nyangaresi VO, Jasim HM, Ma J, Hussain MA, Hussien ZA, Aldarwish AJ. Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture. Sustainability. 2023 Jun 28;15(13):10264.

[21] Oteafy SM, Hassanein HS. IoT in the fog: A roadmap for data-centric IoT development. IEEE Communications Magazine. 2018 Mar 15;56(3):157-63.

[22] Li L, Wang Z, Li N. Efficient attribute-based encryption outsourcing scheme with user and attribute revocation for fog-enabled IoT. IEEE Access. 2020 Sep 18;8:176738-49.

[23] Tu S, Waqas M, Huang F, Abbas G, Abbas ZH. A revocable and outsourced multi-authority attribute-based encryption scheme in fog computing. Computer Networks. 2021 Aug 4;195:108196.

[24] Tange K, De Donno M, Fafoutis X, Dragoni N. A systematic survey of industrial Internet of Things security: Requirements and fog computing opportunities. IEEE Communications Surveys & Tutorials. 2020 Jul 22;22(4):2489-520.

[25] Nyangaresi VO, Yenurkar GK. Anonymity preserving lightweight authentication protocol for resource-limited wireless sensor networks. High-Confidence Computing. 2023 Nov 24:100178.

[26] Tang B, Chen Z, Hefferman G, Wei T, He H, Yang Q. A hierarchical distributed fog computing architecture for big data analysis in smart cities. InProceedings of the ASE BigData & SocialInformatics 2015 2015 Oct 7 (pp. 1-6).

[27] Marston S, Li Z, Bandyopadhyay S, Zhang J, Ghalsasi A. Cloud computing—The business perspective. Decision support systems. 2011 Apr 1;51(1):176-89.

[28] 5Oke AE, Kineber AF, Al-Bukhari I, Famakin I, Kingsley C. Exploring the benefits of cloud computing for sustainable construction in Nigeria. Journal of Engineering, Design and Technology. 2023 Jul 4;21(4):973-90.

[29] Katal A, Dahiya S, Choudhury T. Energy efficiency in cloud computing data centers: a survey on software technologies. Cluster Computing. 2023 Jun;26(3):1845-75.

[30] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan;13(2):691.

[31] Khan S, Parkinson S, Qin Y. Fog computing security: a review of current applications and security solutions. Journal of Cloud Computing. 2017 Dec;6(1):1-22.

[32] Parkinson S, Ward P, Wilson K, Miller J. Cyber threats facing autonomous and connected vehicles: Future challenges. IEEE transactions on intelligent transportation systems. 2017 Mar 6;18(11):2898-915.

[33] Stojmenovic I, Wen S. The fog computing paradigm: Scenarios and security issues. In2014 federated conference on computer science and information systems 2014 Sep 7 (pp. 1-8). IEEE.

[34] Angel NA, Ravindran D, Vincent PD, Srinivasan K, Hu YC. Recent advances in evolving computing paradigms: Cloud, edge, and fog technologies. Sensors. 2021 Dec 28;22(1):196.

[35] Nyangaresi VO. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing. 2023 Sep 15:100154.

[36] Lai Y, Zhang L, Yang F, Zheng L, Wang T, Li KC. CASQ: Adaptive and cloud-assisted query processing in vehicular sensor networks. Future Generation Computer Systems. 2019 May 1;94:237-49.

[37] Jain A, Patel H, Nagalapatti L, Gupta N, Mehta S, Guttula S, Mujumdar S, Afzal S, Sharma Mittal R, Munigala V. Overview and importance of data quality for machine learning tasks. InProceedings of the 26th ACM SIGKDD international conference on knowledge discovery & data mining 2020 Aug 23 (pp. 3561-3562).

[38] Gupta N, Mujumdar S, Patel H, Masuda S, Panwar N, Bandyopadhyay S, Mehta S, Guttula S, Afzal S, Sharma Mittal R, Munigala V. Data quality for machine learning tasks. InProceedings of the 27th ACM SIGKDD conference on knowledge discovery & data mining 2021 Aug 14 (pp. 4040-4041).

[39] Honi DG, Ali AH, Abduljabbar ZA, Ma J, Nyangaresi VO, Mutlaq KA, Umran SM. Towards Fast Edge Detection Approach for Industrial Products. In2022 IEEE 21st International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS) 2022 Dec 19 (pp. 239-244). IEEE.

[40] Rath M, Pati B, Pattanayak BK. Mobile agent-based improved traffic control system in VANET. Integrated Intelligent Computing, Communication and Security. 2019:261-9.

[41] Bangare ML, Bangare PM, Apare RS, Bangare SL. fog computing based security of IoT application. Design Engineering. 2021 Aug 8;7:7542-9.

[42] Mostafavi S, Shafik W. Fog computing architectures, privacy and security solutions. Journal of Communications Technology, Electronics and Computer Science. 2019 Jul 29;24:1-4.

[43] Eid MM, Arunachalam R, Sorathiya V, Lavadiya S, Patel SK, Parmar J, Delwar TS, Ryu JY, Nyangaresi VO, Zaki Rashed AN. QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications. 2022 Jan 17(0).

[44] Kumari S, Singh S. Fog computing: Characteristics and challenges. International Journal of Emerging Trends & Technology in Computer Science. 2017;6(2):113-7.

[45] Yi S, Qin Z, Li Q. Security and privacy issues of fog computing: A survey. InWireless Algorithms, Systems, and Applications: 10th International Conference, WASA 2015, Qufu, China, August 10-12, 2015, Proceedings 10 2015 (pp. 685-695). Springer International Publishing.

[46] Kaur M, Bharti M. Securing user data on cloud using Fog computing and Decoy technique. International Journal of Advance Research in Computer Science and Management Studies. 2014 Oct;2(10):104-10.

[47] Bittencourt L, Immich R, Sakellariou R, Fonseca N, Madeira E, Curado M, Villas L, DaSilva L, Lee C, Rana O. The internet of things, fog and cloud continuum: Integration and challenges. Internet of Things. 2018 Oct 1;3:134-55.

[48] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. InIoT as a Service: 7th EAI International Conference, IoTaaS 2021, Sydney, Australia, December 13–14, 2021, Proceedings 2022 Jul 8 (pp. 3-18). Cham: Springer International Publishing.

[49] Sonmez C, Ozgovde A, Ersoy C. Edgecloudsim: An environment for performance evaluation of edge computing systems. Transactions on Emerging Telecommunications Technologies. 2018 Nov;29(11):e3493.

[50] Premsankar G, Di Francesco M, Taleb T. Edge computing for the Internet of Things: A case study. IEEE Internet of Things Journal. 2018 Feb 12;5(2):1275-84.

[51] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[52] Bonomi F, Milito R, Zhu J, Addepalli S. Fog computing and its role in the internet of things. InProceedings of the first edition of the MCC workshop on Mobile cloud computing 2012 Aug 17 (pp. 13-16).

[53] Anawar MR, Wang S, Azam Zia M, Jadoon AK, Akram U, Raza S. Fog computing: An overview of big IoT data analytics. Wireless Communications and Mobile Computing. 2018 May 7;2018.

[54] Bonomi F, Milito R, Zhu J, Addepalli S. Fog computing and its role in the internet of things. InProceedings of the first edition of the MCC workshop on Mobile cloud computing 2012 Aug 17 (pp. 13-16).

[55] Atieh AT. The next generation cloud technologies: a review on distributed cloud, fog and edge computing and their opportunities and challenges. ResearchBerg Review of Science and Technology. 2021 Oct 9;1(1):1-5.

[56] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1;142:103117.

[57] Jaiswal R, Davidrajuh R, Rong C. Fog computing for realizing smart neighborhoods in smart grids. Computers. 2020 Sep 21;9(3):76.

[58] Hussain MM, Beg MS, Alam MS. Fog computing for big data analytics in IoT aided smart grid networks. Wireless Personal Communications. 2020 Oct;114(4):3395-418.

[59] Basir R, Qaisar S, Ali M, Aldwairi M, Ashraf MI, Mahmood A, Gidlund M. Fog computing enabling industrial internet of things: State-of-the-art and research challenges. Sensors. 2019 Nov 5;19(21):4807.

[60] Ni J, Zhang K, Lin X, Shen X. Securing fog computing for internet of things applications: Challenges and solutions. IEEE Communications Surveys & Tutorials. 2017 Oct 12;20(1):601-28.

[61] Abduljabbar ZA, Omollo Nyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, Qays Abduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19;11(3):55.

[62] Hu P, Dhelim S, Ning H, Qiu T. Survey on fog computing: architecture, key technologies, applications and open issues. Journal of network and computer applications. 2017 Nov 15;98:27-42.

[63] Omoniwa B, Hussain R, Javed MA, Bouk SH, Malik SA. Fog/edge computing-based IoT (FECIoT): Architecture, applications, and research issues. IEEE Internet of Things Journal. 2018 Oct 11;6(3):4118-49.

[64] Hong CH, Varghese B. Resource management in fog/edge computing: a survey on architectures, infrastructure, and algorithms. ACM Computing Surveys (CSUR). 2019 Sep 13;52(5):1-37.

[65] Laroui M, Nour B, Moungla H, Cherif MA, Afifi H, Guizani M. Edge and fog computing for IoT: A survey on current research activities & future directions. Computer Communications. 2021 Dec 1;180:210-31.

[66] Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Khalefa MS, Honi DG. MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones. InFuture Access Enablers for Ubiquitous and Intelligent Infrastructures: 6th EAI International Conference, FABULOUS 2022, Virtual Event, May 4, 2022, Proceedings 2022 Sep 18 (pp. 16-36). Cham: Springer International Publishing.

[67] Gia TN, Rahmani AM, Westerlund T, Liljeberg P, Tenhunen H. Fog computing approach for mobility support in internet-of-things systems. IEEE Access. 2018 Jun 15;6:36064-82.

[68] Mahmood Z, Ramachandran M. Fog computing: Concepts, principles and related paradigms. InFog computing: concepts, frameworks and technologies 2018 Jul 13 (pp. 3-21). Cham: Springer International Publishing.

[69] Naha RK, Garg S, Georgakopoulos D, Jayaraman PP, Gao L, Xiang Y, Ranjan R. Fog computing: Survey of trends, architectures, requirements, and research directions. IEEE access. 2018 Aug 22;6:47980-8009.

[70] Javadzadeh G, Rahmani AM. Fog computing applications in smart cities: A systematic survey. Wireless Networks. 2020 Feb;26(2):1433-57.

[71] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[72] Hazra A, Rana P, Adhikari M, Amgoth T. Fog computing for next-generation internet of things: fundamental, state-of-the-art and research challenges. Computer Science Review. 2023 May 1;48:100549.

[73] Ahlawat C, Krishnamurthi R. Towards smart technologies with integration of the internet of things, cloud computing, and fog computing. International Journal of Networking and Virtual Organisations. 2023;29(1):73-124.

[74] Qureshi R, Asad M, Tunio S, Qureshi S, Ahmed M, Ghulam A. A Survey on Security Issues and Attacks of Fog Computing. VFAST Transactions on Software Engineering. 2023 Jan; 11(1):1-11.

[75] Kürtünlüoğlu P, Akdik B, Karaarslan E. Security of virtual reality authentication methods in metaverse: An overview. arXiv preprint arXiv:2209.06447. 2022 Sep 14.

[76] Singh PD, Singh KD. Security and Privacy in Fog/Cloud-based IoT Systems for AI and Robotics. EAI Endorsed Transactions on AI and Robotics. 2023 Aug 28;2.

[77] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InApplied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings 2022 Oct 6 (pp. 46-64). Cham: Springer Nature Switzerland.

[78] Das R, Inuwa MM. A review on fog computing: issues, characteristics, challenges, and potential applications. Telematics and Informatics Reports. 2023 Feb 28:100049.

[79] Patil, K., Gupta, S., Nair, A., & Gutte, V. Cloud, Fog and Edge Computing: Security and Privacy Concerns. International Journal for Research in Applied Science and Engineering Technology. 2022 Jun; 10(5): 286–291.

[80] Ashi Z, Al-Fawa'reh M, Al-Fayoumi M. Fog computing: security challenges and countermeasures. Int. J. Comput. Appl. 2020 Aug;175(15):30-6.

[81] Gautam V, Lanjewar U. Fog Computing: Analyzing Challenges, Unveiling Opportunities, and Maximizing Benefits. International Journal for Research in Applied Science and Engineering Technology. 2022, Feb; 10(7): 4008–4012.

[82] Alzoubi YI, Osmanaj VH, Jaradat A, Al-Ahmad A. Fog computing security and privacy for the Internet of Thing applications: State-of-the-art. Security and Privacy. 2021 Mar;4(2):e145.

[83] Singh J, Singh P, Gill SS. Fog computing: A taxonomy, systematic review, current trends and research challenges. Journal of Parallel and Distributed Computing. 2021 Nov 1;157:56-85.

[84] Alzoubi YI, Al-Ahmad A, Jaradat A. Fog computing security and privacy issues, open challenges, and blockchain solution: An overview. International Journal of Electrical & Computer Engineering (2088-8708). 2021 Dec 1;11(6).

[85] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[86] Bin S, Yongjie W. Key Technologies of Security Access Control in Fog Computing Environment. InJournal of Physics: Conference Series 2021 Jul 1 (Vol. 1982, No. 1, p. 012188). IOP Publishing.

[87] Singh JK, kumar Goel A. Study on fog computing: security & privacy challenges in terms of IoT. InJournal of Physics: Conference Series 2021 Aug 1 (Vol. 2007, No. 1, p. 012039). IOP Publishing.

[88] Hasan RT, Ameen SY. Security enhancement of iot and fog computing via blockchain applications. Journal of Soft Computing and Data Mining. 2021 Oct 24;2(2):26-38.

[89] Al Harbi S, Halabi T, Bellaiche M. Fog computing security assessment for device authentication in the internet of things. In2020 IEEE 22nd International Conference on High Performance Computing and Communications; IEEE 18th International Conference on Smart City; IEEE 6th International Conference on Data Science and Systems (HPCC/SmartCity/DSS) 2020 Dec 14 (pp. 1219-1224). IEEE.

[90] Arivazhagan C, Natarajan V. A Survey on Fog computing paradigms, Challenges and Opportunities in IoT. In2020 International Conference on Communication and Signal Processing (ICCSP) 2020 Jul 28 (pp. 0385-0389). IEEE.

[91] Alli AA, Alam MM. The fog cloud of things: A survey on concepts, architecture, standards, tools, and applications. Internet of Things. 2020 Mar 1;9:100177.

[92] Khan S, Parkinson S, Qin Y. Fog computing security: a review of current applications and security solutions. Journal of Cloud Computing. 2017 Dec;6(1):1-22.

[93] Gope P. LAAP: Lightweight anonymous authentication protocol for D2D-aided fog computing paradigm. computers & security. 2019 Sep 1;86:223-37.

[94] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[95] Aljumah A, Ahanger TA. Fog computing and security issues: A review. In2018 7th international conference on computers communications and control (ICCCC) 2018 May 8 (pp. 237-239). IEEE.

[96] Kayes AS, Rahayu W, Watters P, Alazab M, Dillon T, Chang E. Achieving security scalability and flexibility using fog-based context-aware access control. Future Generation Computer Systems. 2020 Jun 1;107:307-23.

[97] Parikh S, Dave D, Patel R, Doshi N. Security and privacy issues in cloud, fog and edge computing. Procedia Computer Science. 2019 Jan 1;160:734-9.

[98] Kayes AS, Rahayu W, Watters P, Alazab M, Dillon T, Chang E. Achieving security scalability and flexibility using fog-based context-aware access control. Future Generation Computer Systems. 2020 Jun 1;107:307-23.

[99] Garg R, Varadi S, Kertész A. Legal considerations of IoT applications in fog and cloud environments. In2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP) 2019 Feb 13 (pp. 193-198). IEEE.

[100] Amor AB, Abid M, Meddeb A. A secure fog-based communication scheme. In2017 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC) 2017 Oct 20 (pp. 146-151). IEEE.

[101] Ferretti L, Marchetti M, Colajanni M. Fog-based secure communications for low-power IoT devices. ACM Transactions on Internet Technology (TOIT). 2019 Mar 28;19(2):1-21.

[102] Patil Abhijit J, Syam Prasad G. Trust based security model for IoT and fog based applications, International Journal of Engineering and Technology (UAE). vol. 2018;7:691-5.

[103] Umran SM, Lu S, Abduljabbar ZA, Nyangaresi VO. Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet of Things. 2023 Dec 1;24:100969.

[104] Gupta M, Sandhu R. Authorization framework for secure cloud assisted connected cars and vehicular internet of things. InProceedings of the 23nd ACM on symposium on access control models and technologies 2018 Jun 7 (pp. 193-204).

[105] Xu Q, Tan C, Fan Z, Zhu W, Xiao Y, Cheng F. Secure data access control for fog computing based on multi-authority attribute-based signcryption with computation outsourcing and attribute revocation. Sensors. 2018 May 17;18(5):1609.

[106] Martin BA, Michaud F, Banks D, Mosenia A, Zolfonoon R, Irwan S, Schrecker S, Zao JK. OpenFog security requirements and approaches. In2017 IEEE Fog World Congress (FWC) 2017 Oct 30 (pp. 1-6). IEEE.

[107] Sharma P, Prasad R. Techniques for Implementing Fault Tolerance in Modern Software Systems to Enhance Availability, Durability, and Reliability. Eigenpub Review of Science and Technology. 2023 Sep 18;7(1):239-51.

[108] Khan MM, Nencioni G. Resource Allocation in Networking and Computing Systems: a Security and Dependability Perspective. IEEE Access. 2023 Aug 18.

[109] Al-Chaab W, Abduljabbar ZA, Abood EW, Nyangaresi VO, Mohammed HM, Ma J. Secure and Low-Complexity Medical Image Exchange Based on Compressive Sensing and LSB Audio Steganography. Informatica. 2023 May 31;47(6).

[110] Hussain Y, Huang Z. TRFIoT: Trust and reputation model for fog-based IoT. InCloud Computing and Security: 4th International Conference, ICCCS 2018, Haikou, China, June 8-10, 2018, Revised Selected Papers, Part VI 4 2018 (pp. 187-198). Springer International Publishing.

[111] Dang TD, Hoang D. A data protection model for fog computing. In2017 Second International Conference on Fog and Mobile Edge Computing (FMEC) 2017 May 8 (pp. 32-38). IEEE.

[112] Sankar SM, Revathi ST, Thiagarajan R. Hybrid Authentication Using Node Trustworthy to Detect Vulnerable Nodes. Computer Systems Science & Engineering. 2023 Apr 1;45(1).

[113] Wei P, Wang D, Zhao Y, Tyagi SK, Kumar N. Blockchain data-based cloud data integrity protection mechanism. Future Generation Computer Systems. 2020 Jan 1;102:902-11.

[114] Patwary AA, Fu A, Naha RK, Battula SK, Garg S, Patwary MA, Aghasian E. Authentication, access control, privacy, threats and trust management towards securing fog computing environments: A review. arXiv preprint arXiv:2003.00395. 2020 Mar 1.

[115] Abdallah HA, Meshoul S. A Multilayered Audio Signal Encryption Approach for Secure Voice Communication. Electronics. 2023 Jan;12(1):2.

[116] Dehalwar V, Kolhe ML, Deoli S, Jhariya MK. Blockchain-based trust management and authentication of devices in smart grid. Cleaner Engineering and Technology. 2022 Jun 1;8:100481.

[117] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[118] Yusof YB, Ping TH, Isa FB. Strengthening Smart Grids Through Security Measures: A Focus on Real-Time Monitoring, Redundancy, and Cross-Sector Collaboration. International Journal of Intelligent Automation and Computing. 2023 Aug 3;6(3):14-36.

[119] Silva FA, Brito C, Araújo G, Fé I, Tyan M, Lee JW, Nguyen TA, Maciel PR. Model-driven impact quantification of energy resource redundancy and server rejuvenation on the dependability of medical sensor networks in smart hospitals. Sensors. 2022 Feb 18;22(4):1595.

[120] Kounoudes AD, Kapitsaki GM. A mapping of IoT user-centric privacy preserving approaches to the GDPR. Internet of Things. 2020 Sep 1;11:100179.

[121] Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023 Mar 11;12(6):1333.

[122] S. Sarkar, S. Chatterjee, and S. Misra, "Sarkar S, Chatterjee S, Misra S. Assessment of the Suitability of Fog Computing in the Context of Internet of Things. IEEE Transactions on Cloud Computing. 2015 Oct 1;6(1):46-59.

[123] Stojmenovic I, Wen S, Huang X, Luan H. An overview of fog computing and its security issues. Concurrency and Computation: Practice and Experience. 2016 Jul;28(10):2991-3005.

[124] Puliafito C, Mingozzi E, Longo F, Puliafito A, Rana O. Fog computing for the internet of things: A survey. ACM Transactions on Internet Technology (TOIT). 2019 Apr 2;19(2):1-41.

[125] Zhou J, Lin X, Dong X, Cao Z. PSMPA: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributedm-healthcare cloud computing system. IEEE transactions on parallel and distributed systems. 2014 Mar 27;26(6):1693-703.

[126] Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E, Markakis EK. A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. IEEE Communications Surveys & Tutorials. 2020 Jan 6;22(2):1191-221.

[127] Rauti S, Laato S. Understanding software obfuscation and diversification as defensive measures for the cybersecurity of Internet of Things. InHawaii International Conference on System Sciences 2023 (pp. 6645-6654).

[128] Al-Sulami ZA, Abduljabbar ZA, Nyangaresi VO, Ma J. Knowledge Management and its Role in the Development of a Smart University in Iraq. TEM Journal. 2023 Aug 1;12(3):1582.

[129] Tiburski RT, de Matos E, Hessel F. Evaluating the dtls protocol from coap in fog-to-fog communications. In2019 IEEE International Conference on Service-Oriented System Engineering (SOSE) 2019 Apr 4 (pp. 90-905). IEEE.

[130] Rezapour R, Asghari P, Javadi HH, Ghanbari S. Security in fog computing: A systematic review on issues, challenges and solutions. Computer Science Review. 2021 Aug 1;41:100421.

[131] Maheswari KU, Bhanu SM, Savarimuthu N. Clustering-based data integrity verification approach for multi-replica in a fog environment. The Journal of Supercomputing. 2023 Aug 28:1-25.

[132] Yang Y, Luo X, Chu X, Zhou MT, Yang Y, Luo X, Chu X, Zhou MT. Fog computing architecture and technologies. Fog-Enabled Intelligent IoT Systems. 2020:39-60.

[133] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access. 2022 Feb 11;10:26257-70.

[134] Martinez I, Hafid AS, Jarray A. Design, resource management, and evaluation of fog computing systems: a survey. IEEE Internet of Things Journal. 2020 Sep 11;8(4):2494-516.

[135] Kumari P, Jain AK. A comprehensive study of DDoS attacks over IoT network and their countermeasures. Computers & Security. 2023 Jan 13:103096.

[136] Chang V, Golightly L, Modesti P, Xu QA, Doan LM, Hall K, Boddu S, Kobusińska A. A survey on intrusion detection systems for fog and cloud computing. Future Internet. 2022 Mar 13;14(3):89.

[137] Gola KK, Arya S, Khan G, Devkar C, Chaurasia N. Security analysis of fog computing environment for ensuring the security and privacy of information. Transactions on Emerging Telecommunications Technologies. 2023 Oct;34(10):e4861.

[138] Alazeb A, Panda B, Almakdi S, Alshehri M. Data integrity preservation schemes in smart healthcare systems that use fog computing distribution. Electronics. 2021 May 30;10(11):1314.

[139] Soleymani SA, Goudarzi S, Anisi MH, Zareei M, Abdullah AH, Kama N. A security and privacy scheme based on node and message authentication and trust in fog-enabled VANET. Vehicular Communications. 2021 Jun 1;29:100335.

[140] Aleisa MA, Abuhussein A, Sheldon FT. Access control in fog computing: Challenges and research agenda. IEEE Access. 2020 May 5;8:83986-99.

[141] Nyangaresi VO, Ibrahim A, Abduljabbar ZA, Hussain MA, Al Sibahee MA, Hussien ZA, Ghrabat MJ. Provably Secure Session Key Agreement Protocol for Unmanned Aerial Vehicles Packet Exchanges. In2021 International Conference on Electrical, Computer and Energy Technologies (ICECET) 2021 Dec 9 (pp. 1-6). IEEE.

[142] Mamonov S, Benbunan-Fich R. The impact of information security threat awareness on privacy-protective behaviors. Computers in Human Behavior. 2018 Jun 1;83:32-44.

[143] Salim MM, Rathore S, Park JH. Distributed denial of service attacks and its defenses in IoT: a survey. The Journal of Supercomputing. 2020 Jul;76:5320-63.

[144] Farhadi M, Lanet JL, Pierre G, Miorandi D. A systematic approach toward security in Fog computing: Assets, vulnerabilities, possible countermeasures. Software: Practice and Experience. 2020 Jun;50(6):973-97.

[145] van Daalen OL. The right to encryption: Privacy as preventing unlawful access. Computer Law & Security Review. 2023 Jul 1;49:105804.

[146] Noura M, Atiquzzaman M, Gaedke M. Interoperability in internet of things: Taxonomies and open challenges. Mobile networks and applications. 2019 Jun 15;24:796-809.

[147] Senapati KK, Kumar A, Sinha K. Impact of Information Leakage and Conserving Digital Privacy. InMalware Analysis and Intrusion Detection in Cyber-Physical Systems 2023 (pp. 166-188). IGI Global.

[148] Abood EW, Abdullah AM, Al Sibahe MA, Abduljabbar ZA, Nyangaresi VO, Kalafy SA, Ghrabta MJ. Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics. 2022 Feb 1;11(1):185-94.

[149] Sandvik JP, Franke K, Abie H, Årnes A. Evidence in the fog–Triage in fog computing systems. Forensic Science International: Digital Investigation. 2023 Mar 1;44:301506.

[150] Mukherjee M, Shu L, Wang D. Survey of fog computing: Fundamental, network applications, and research challenges. IEEE Communications Surveys & Tutorials. 2018 Mar 12;20(3):1826-57.

[151] Zahra SR, Chishti MA. A generic and lightweight security mechanism for detecting malicious behavior in the uncertain Internet of Things using fuzzy logic-and fog-based approach. Neural Computing and Applications. 2022 May;34(9):6927-52.

[152] Tan SF, Samsudin A. Recent technologies, security countermeasure and ongoing challenges of Industrial Internet of Things (IIoT): A survey. Sensors. 2021 Oct 6;21(19):6647.

[153] Al Sibahee MA, Abdulsada AI, Abduljabbar ZA, Ma J, Nyangaresi VO, Umran SM. Lightweight, Secure, Similar-Document Retrieval over Encrypted Data. Applied Sciences. 2021 Jan;11(24):12040.

[154] Brasser F, Rasmussen KB, Sadeghi AR, Tsudik G. Remote attestation for low-end embedded devices: the prover's perspective. InProceedings of the 53rd Annual Design Automation Conference 2016 Jun 5 (pp. 1-6).

[155] Marasco E, Albanese M, Patibandla VV, Vurity A, Sriram SS. Biometric multi-factor authentication: On the usability of the FingerPIN scheme. Security and Privacy. 2023 Jan;6(1):e261.

[156] Suleski T, Ahmed M, Yang W, Wang E. A review of multi-factor authentication in the Internet of Healthcare Things. Digital Health. 2023 May;9:20552076231177144.

[157] Zaenchkovski A, Lazarev A, Masyutin S. Multi-factor Authentication in Innovative Business Systems of Industrial Clusters. InInternational Russian Automation Conference 2022 Sep 4 (pp. 271-281). Cham: Springer International Publishing.

[158] Mohammed AH, Dziyauddin RA, Latiff LA. Current Multi-factor of Authentication: Approaches, Requirements, Attacks and Challenges. International Journal of Advanced Computer Science and Applications. 2023;14(1).

[159] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[160] Kayes AS, Kalaria R, Sarker IH, Islam MS, Watters PA, Ng A, Hammoudeh M, Badsha S, Kumara I. A survey of context-aware access control mechanisms for cloud and fog networks: Taxonomy and open research issues. Sensors. 2020 Apr 27;20(9):2464.

[161] Daoud WB, Obaidat MS, Meddeb-Makhlouf A, Zarai F, Hsiao KF. TACRM: trust access control and resource management mechanism in fog computing. Human-centric Computing and Information Sciences. 2019 Dec;9(1):1-8.

[162] Benlloch-Caballero P, Wang Q, Calero JM. Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks. Computer Networks. 2023 Feb 1;222:109526.

[163] Ometov A, Molua OL, Komarov M, Nurmi J. A survey of security in cloud, edge, and fog computing. Sensors. 2022 Jan 25;22(3):927.

[164] Itoo S, Ahmad M, Kumar V, Alkhayyat A. RKMIS: robust key management protocol for industrial sensor network system. The Journal of Supercomputing. 2023 Jan 21:1-29.

[165] Bhardwaj A, Surmani Martins MV, You Y, Sajja R, Rimmer M, Goutham S, Qi R, Abbas Dar S, Radha B, Keerthi A. Fabrication of angstrom-scale two-dimensional channels for mass transport. Nature Protocols. 2023 Nov 27:1-41.

[166] Nyakomitta SP, Omollo V. Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE). 2014;16(5):137-44.

[167] Khader M, Karam M. Assessing the Effectiveness of Masking and Encryption in Safeguarding the Identity of Social Media Publishers from Advanced Metadata Analysis. Data. 2023 Jun 13;8(6):105.

[168] Cadavid JA. The Origin and Purpose of Legal Protection for the Integrity of Copyright Metadata. IIC-International Review of Intellectual Property and Competition Law. 2023 Sep;54(8):1179-202.

[169] Ross GM, Zhao Y, Bosman AJ, Geballa-Koukoula A, Zhou H, Elliott CT, Nielen MW, Rafferty K, Salentijn GI. Best practices and current implementation of emerging smartphone-based (bio) sensors–Part 1: Data handling and ethics. TrAC Trends in Analytical Chemistry. 2023 Jan 1;158:116863.

[170] Reer A, Wiebe A, Wang X, Rieger JW. FAIR human neuroscientific data sharing to advance AI driven research and applications: Legal frameworks and missing metadata standards. Frontiers in Genetics. 2023 Mar 13;14:1086802.

[171] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1;133:102763.

[172] Korus P. Digital image integrity–a survey of protection and verification techniques. Digital Signal Processing. 2017 Dec 1;71:1-26.

[173] Kitchin R, Dodge M. The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. InSmart Cities and Innovative Urban Technologies 2020 Dec 29 (pp. 47-65). Routledge.

[174] Nunes M, Abreu A, Bagnjuk J, Nunes E, Saraiva C. A Strategic Process to Manage Collaborative Risks in Supply Chain Networks (SCN) to Improve Resilience and Sustainability. Sustainability. 2022 Apr 26;14(9):5237.

[175] Wang Y, Rousis AO, Strbac G. On microgrids and resilience: A comprehensive review on modeling and operational strategies. Renewable and Sustainable Energy Reviews. 2020 Dec 1;134:110313.

[176] Statsenko L, Jayasinghe RS, Soosay C. Supply network resilience capabilities: a social–ecological perspective. Supply Chain Management: An International Journal. 2023 Aug 8.

[177] Abood EW, Hussien ZA, Kawi HA, Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Kalafy A, Ahmad S. Provably secure and efficient audio compression based on compressive sensing. International Journal of Electrical & Computer Engineering (2088-8708). 2023 Feb 1;13(1).

[178] Khater BS, Abdul Wahab AW, Idris MY, Hussain MA, Ibrahim AA, Amin MA, Shehadeh HA. Classifier performance evaluation for lightweight IDS using fog computing in IoT security. Electronics. 2021 Jul 8;10(14):1633.

[179] Ding Z, He D, Qiao Q, Li X, Gao Y, Chan S, Choo KK. A Lightweight and Secure Communication Protocol for the IoT Environment. IEEE Transactions on Dependable and Secure Computing. 2023 Apr 17.

[180] Aliya B, Olga U, Yenlik B, Sogukpinar I. Ensuring Information Security of Web Resources Based on Blockchain Technologies. International Journal of Advanced Computer Science and Applications. 2023;14(6).

[181] Carrillo-Torres D, Pérez-Díaz JA, Cantoral-Ceballos JA, Vargas-Rosales C. A Novel Multi-Factor Authentication Algorithm Based on Image Recognition and User Established Relations. Applied Sciences. 2023 Jan 20;13(3):1374.

[182] More D, Deore B, Bhosale S. Multifactor Biometric Authentication for Cloud Computing Security. InProceedings of International Conference on Communication and Artificial Intelligence: ICCAI 2021 2022 May 10 (pp. 389-397). Singapore: Springer Nature Singapore.

[183] Abduljaleel IQ, Abduljabbar ZA, Al Sibahee MA, Ghrabat MJ, Ma J, Nyangaresi VO. A Lightweight Hybrid Scheme for Hiding Text Messages in Colour Images Using LSB, Lah Transform and Chaotic Techniques. Journal of Sensor and Actuator Networks. 2022 Dec;11(4):66.

[184] Dixit R, Ravindranath K. Enhancement in Security for Intercloud Scenario with the Help of Role-Based Access Control Model. InIOT with Smart Systems: Proceedings of ICTIS 2021, Volume 2 2022 (pp. 277-285). Springer Singapore.

[185] Li J, Tu T, Li Y, Qin S, Shi Y, Wen Q. DoSGuard: Mitigating denial-of-service attacks in software-defined networks. Sensors. 2022 Jan 29;22(3):1061.

[186] Martyshkin AI, Biktashev RA. Research and Analysis of Computing Cluster Configuration Management Systems. InInternational Russian Automation Conference 2022 Sep 4 (pp. 194-205). Cham: Springer International Publishing.

[187] Thapliyal S, Wazid M, Singh DP, Das AK, Shetty S, Alqahtani A. Design of robust Blockchain-envisioned authenticated key management mechanism for smart healthcare applications. IEEE Access. 2023 Aug 30.

[188] Bettayeb S, Messai ML, Hemam SM. A robust and efficient vector-based key management scheme for IoT networks. Ad Hoc Networks. 2023 Oct 1;149:103250.

[189] Nyangaresi VO, Abd-Elnaby M, Eid MM, Nabih Zaki Rashed A. Trusted authority based session key agreement and authentication algorithm for smart grid networks. Transactions on Emerging Telecommunications Technologies. 2022 Sep;33(9):e4528.

[190] Ali Z, Mahmood A, Khatoon S, Alhakami W, Ullah SS, Iqbal J, Hussain S. A generic Internet of Things (IoT) middleware for smart city applications. Sustainability. 2023 Jan;15(1):743.

[191] Zuo Z, Watson M, Budgen D, Hall R, Kennelly C, Al Moubayed N. Data anonymization for pervasive health care: systematic literature mapping study. JMIR medical informatics. 2021 Oct 15;9(10):e29871.

[192] Buccafurri F, De Angelis V, Lazzaro S. Enabling anonymized open-data linkage by authorized parties. Journal of Information Security and Applications. 2023 May 1;74:103478.

[193] Tomás J, Rasteiro D, Bernardino J. Data anonymization: an experimental evaluation using open-source tools. Future Internet. 2022 May 30;14(6):167.

[194] Hussain MA, Hussien ZA, Abduljabbar ZA, Ma J, Al Sibahee MA, Hussain SA, Nyangaresi VO, Jiao X. Provably throttling SQLI using an enciphering query and secure matching. Egyptian Informatics Journal. 2022 Dec 1; 23(4):145-62.

[195] Sheeraz M, Paracha MA, Haque MU, Durad MH, Mohsin SM, Band SS, Mosavi A. Effective Security Monitoring Using Efficient SIEM Architecture. Hum.-Centric Comput. Inf. Sci. 2023 Apr 30;13:1-8.

[196] Fatima A, Khan TA, Abdellatif TM, Zulfiqar S, Asif M, Safi W, Al Hamadi H, Al-Kassem AH. Impact and Research Challenges of Penetrating Testing and Vulnerability Assessment on Network Threat. In2023 International Conference on Business Analytics for Technology and Security (ICBATS) 2023 Mar 7 (pp. 1-8). IEEE.

[197] Malhotra A, Elsayed A, Torres R, Venkatraman S. Evaluate Solutions for Achieving High Availability or Near Zero Downtime for Cloud Native Enterprise Applications. IEEE Access. 2023 Aug 9.