Journal of Theoretical and Applied Information Technology
30th November 2024. Vol.102. No. 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN EXTENSIVE REVIEW OF SECURITY ISSUES AND CHALLENGES IN FOG COMPUTING ENVIRONMENT

W. ALGESHARI[1], M. SHER. RAMAZAN[2], F. ALOTAIBI[3], K. ALYOUBI[4]

[1]designation, Faculty Of Computing And Information Technology, Department Of Information System, King Abdul Aziz University, Jeddah, Saudi Arabia
[2]designation, Faculty Of Computing And Information Technology, Department Of Information System, King Abdul Aziz University, Jeddah, Saudi Arabia
[3]designation, Faculty Of Computing And Information Technology, Department Of Information System, King Abdul Aziz University, Jeddah, Saudi Arabia
[4]designation, Faculty Of Computing And Information Technology, Department Of Information System, King Abdul Aziz University, Jeddah, Saudi Arabia
E-mail: [1]algeshari@stu.kau.edu.sa ,[2] msramadan@kau.edu.sa, [3]fsalotaibi@kau.edu.sa , [4]kalyoubi@kau.edu.sa

ABSTRACT

As a crucial addition to cloud computing, fog computing provides localized processing resources and services near end devices at the network edge. The drawbacks of traditional cloud computing, like excessive latency, immobility, and poor location awareness, are addressed by this design, which is especially advantageous for the Internet of Things (IoT). Despite its advantages, fog computing poses serious security risks because of its decentralized architecture, close proximity to end users, and confined processing power. These security issues become more serious as IoT device counts rise, increasing the possibility of cyberattacks. This review article offers an extensive overview of the security issues and challenges unique to fog computing systems. It outlines various attack vectors, examines the design, traits, and vulnerabilities of fog nodes, and addresses mitigating these risks with countermeasures. This paper attempts to identify important security issues in fog computing and suggest future strategies for resolving these issues to ensure safe and reliable fog-IoT ecosystems by assessing previous research.

Keywords: *IOT, Cloud Computing, FOG Computing, FOG Attacks*

1. INTRODUCTION

Over the past ten years, the Internet of Things (IoT) has been widely implemented in a variety of application areas, and in the years to come, its ubiquity will only increase. The IoT industry is anticipated to expand by 75 billion by 2025 [1]. According to the latest report of the statista[1] by 2030, there will be approximately 32.1 billion IoT devices globally, almost doubling from 15.9 billion in 2023. China is expected to lead the world with almost 8 billion consumer IoT devices by 2033. About 60 % of all IoT devices were consumer devices in 2023; this percentage is expected to stay constant over the following ten years. There are presently over 100 million connected IoT devices in each of the following industries: retail, transportation, government, gas, power, and water supply. By 2033, it is anticipated that there will be over 8 billion connected IoT devices worldwide. Key consumer use cases include connected cars, IT infrastructure, asset tracking, and smart grid applications, as well as internet and media devices like smartphones, which are predicted to reach over 17 billion units by 2033. The concept of IoT allows for control and communication across a vast array of different devices. By connecting equipment such as communication devices, sensors, and data processing units, IoT provides dispersed, autonomous decision making as well as intelligent data processing and analysis [2]. Applications for IoT based systems can be found in a large range of sectors, including trade, education, healthcare, agriculture, and the military. Due to this broad acceptance, there has been an extraordinary increase in the number of connected devices, which has caused a huge spike in the amount of data being sent to cloud services. In addition to improving operational effectiveness and enabling real time decision making amongst a range of sectors, the

[1]IoT connections worldwide 2022-2033 | Statista

exponential expansion of IoT devices has raised the need for cloud infrastructure in order to handle, process, and analyze the large volumes of data that are generated. Because of this, it is now essential to guarantee reliable and scalable cloud solutions in order to efficiently manage the complexity and volume of IoT traffic [3]. The reliability, accessibility, and effectiveness of data backups are the three most important criteria used to classify an organization data space. The practice of providing computer resources to secure and protect data accessible from unauthorized persons is known as cloud computing. The growing necessity for cloud computing within organizations has presented previously unheard-of information security concerns [4]. Customers can pay for the use of a shared computer resource pool on an as needed or pay per use basis using a cloud computing paradigm. Cloud based computing gives users and companies with numerous advantages in terms of capital investment and operating cost reductions. Even with these advantages, cloud computing acceptance is nevertheless constrained by a number of issues. Security and high latency is an vital issue that is typically considered. Without this crucial element, the computing approach has an adverse effect that causes suffering on an individual level, ethics, and the economy [5]. Fog computing emerged as a response to cloud computing limitations in latency, security, energy consumption and many other notable issues. Coined by Cisco, it represents a distributed computing approach that brings cloud capabilities closer to the network edge. Fog computing enables the management of computing resources, data storage, and network services across fog devices, cloud data centers, and end-user devices [6] [7]. Operating closer to the network edge, fog computing acts as an intermediate between cloud data centers and end users (See Fig. 1). Fog computing reduces the possibility of network attacks by putting storage and processing power closer to endpoints. Using devices like access points, gateways, and local storage, this architecture lowers the energy consumption of large-scale cloud infrastructure while speeding up data processing. As a result, end users no longer exclusively rely on cloud data centers and instead engage with fog devices [8]. Although cloud data centers are protected by strong security protocols, fog devices have minimum resources, which makes them more prone to cyberattacks.

1.1 Motivation

Security solutions are not immediately applicable to fog environments, in contrast to cloud computing. As such, the implementation of IoT fog computing demands strong security protocols to guard against its weaknesses [9]. Adversaries use a variety of assault strategies to undermine the availability and integrity of IoT fog computing infrastructure. Denial-of-service (DoS), forgeries, man-in-the-middle (MitM), Sybil attacks, eavesdropping, and impersonation are a few examples of these. The availability, confidentiality, and integrity of critical information and services in the fog environment are seriously threatened by these malicious activities [10][11]. Because of these flaws, malicious users may try to breach fog networks and compromise user data by penetrating the system. A crucial security tool for proactively identifying and countering hostile activity within a network is an intrusion detection system (IDS) [12]. IDS can identify anomalies that point to ongoing attacks, policy violations, or illegal access by continually monitoring network traffic and system behavior. Basic security techniques like intrusion detection and prevention protect systems against online threats. While intrusion prevention seeks to proactively block threats before they can do harm, intrusion detection concentrates on discovering and responding to ongoing attacks [4].

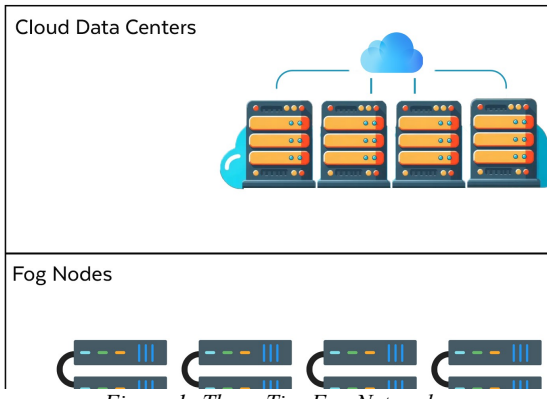

Figure 1: Three-Tier Fog Network

The review paper provides a thorough examination of fog computing security issues, particularly in Internet of Things settings. Fog decentralized architecture and close connection to end users present weaknesses that are highlighted, along with important threats and solutions. Offering insights into future research possibilities, the report covers the growing hazards posed by the swift growth of IoT devices and examines current approaches to secure fog nodes.

1.2 Contribution And Research Goals

This paper presents a thorough overview of fog computing, examines how it integrates with the Internet of Things, and its comparisons with the cloud computing. The goal of this research is to explore the existing methods of cybersecurity by examining the security, functional, and architectural features of fog computing. With a focus on industry-specific applications, the survey examines challenges, risks, and mitigation techniques in fog computing with IoT environment. The research main goal is to discuss the particular attacks and difficulties associated with fog computing especially those that traditional systems might not be able to sufficiently address. Lastly its explores and analyzing current developments in the field to help researchers grasp the most recent developments in fog computing security. The remaining part of the paper has been organized as follows: The background and architecture of Fog Computing and IoT are presented in section: 2. The layer architecture is detailed in the subsection section: 3.1. Key aspects of Fog Computing are discussed in section: 3.2. The security concerns and possible attacks related to Fog Computing are covered in section: 3.3 and section: 3.4. The synergy between fog computing, challenges and issues associated with the fog computing and IoT are highlighted in section: 3.5 and 3.5.1. Finally, the conclusion and potential directions for future work are presented in section: 4.

1.3 Research Methodology

ACM Digital Library, IEEE Xplore, SpringerLink, ScienceDirect, and other reputable academic databases provided data that was carefully gathered for this systematic research. These resources have been selected because they offer thorough and trustworthy compilations of peer-reviewed studies on intrusion detection systems, fog computing, and the internet of things. ”Fog Computing”, ”Internet of Things”, ”Fog Networks”, ”IoT Security” ,”Security Challenges in Fog Computing,” were amongst the most prominent keywords used in the search. Certain filters were used to narrow down the search results, focusing on document kinds such survey papers, review articles, journals, and conference papers as well as publication years from 2000 to 2024. To ensure uniformity and relevance, all searches were carried out in the English language. This research seeks to answer several analytical questions, like:

1. What makes fog computing essential and how does it interact with the Internet of Things?
2. Which fog computing attacks are possible, and what countermeasures have been recommended?
3. What are the possible future directions using artificial intelligence, quantum communication and cryptography?

The research also makes suggestions for potential future improvements to IDS in fog computing systems based on the patterns and issues revealed.

2. BACKGROUND

This section explores the key elements of fog computing and the Internet of Things beginning with examination of the salient features that set fog computing apart from alternative paradigms such as cloud and edge computing. An overview of the IoT environment is also given, along with a look at popular architectures and protocols that are essential to IoT operation. The final section of the article examines the integration of fog computing and IoT, outlining the advantages and difficulties of this alliance. Through this a thorough grasp of how fog computing and the internet of things are intertwined is established.

Cloud computing has completely changed how we store, handle, and process data in the modern digital world. Cloud computing has become the foundation of modern technology, supporting everything from basic web apps to intricate enterprise solutions, by providing scalable, on-demand computing resources over the internet. Because of its centralized control, it has strong data processing skills that have aided in the expansion of services in a number of different companies [13]. However, some of cloud computing limitations (See Table. 1) are now apparent as the number of connected devices keeps rising, especially with the emergence of the Internet of Things [14] [15]. The drawbacks of depending only on centralized cloud infrastructures have become evident due to the enormous amount of data created by IoT devices and the requirement for real-time processing and low-latency responses. Challenges including latency, network congestion, and lack of location awareness pose serious obstacles, particularly in applications where quick data processing is essential [13] [16]. Thus the demand for decentralized computing solutions has increased due to the growth of IoT devices. In response, a potential concept known as edge computing emerged to solve the shortcomings of centralized cloud computing. Edge computing provides lower latency, more bandwidth, and

improved privacy by moving compute and storage closer to data sources [17]. Numerous edge computing paradigms have appeared [18] [19] [20], each providing a distinct approach to distributed computing, such as Mobile Cloud Computing (MCC), Cloudlet Computing (CC), and Mobile Edge Computing (MEC). The ultimate form of edge computing is fog computing, which provides an all-encompassing architecture that disperses resources along the cloud-to-things continuum [21]. Even if it solves issues like latency and bandwidth better than cloud computing, the technology is still developing. Many edge and fog computing ideas have been proposed, but a common understanding is still challenging. To fully exploit these transformational computing paradigms, promise, a significant amount of research and development is required. Around 2004 or 2005, the idea of edge computing first emerged, with an emphasis on moving data and application logic closer to network endpoints [22] [23]. Cloud and IoT emerged into existence shortly following edge computing. Google and Amazon first used the term "cloud computing" in 2006 [24], and in 2008 there was increased scholarly attention to it [25] [26]. Although the idea of IoT has been around since 1999, it was not until 2006 that it started to receive a lot of attention in scholarly journals [27]. By contrast, fog computing has a well-defined history. Flavio Bonomi of Cisco originally brought it up and defined it in 2012 [28]. Fog computing is a new paradigm that disperses processing power closer to data sources than standard cloud computing, which centralizes resources. Software applications and other services can be delivered more effectively owing to this decentralized strategy faster processing and lower latency. This is useful for cloud solutions for high mobility technologies like vehicle ad hoc networks (VANET) and the Internet of Things, Green internet of things (GIoT) and many other notable technologies. In fog computing, devices are typically connected directly to their destination rather than through a convoluted network infrastructure. The connection will therefore have significantly reduced latency and improved quality of service. The Fog Computing System was designed to bridge the service gaps left by Cloud Computing, not to completely replace it [29] [30] [31]. According to Cisco Systems, the fog computing is a virtual platform that provides cloud computing data centers—which are not precisely situated at the network edge—with networking, storage, and processing capabilities for end devices. In order to offer them with services and meet their expectations faster, fog is different from cloud in that it has brought end users closer to it. [32] Whereas fog computing balances central and local computing, storage, and network management, cloud computing transfers computation, control, and storage data to the centralized cloud. Table 1 provides a comparative comparison of fog with the cloud computing. A more seamless customer experience and better management are offered by fog computing.

Table 1: Comparative analysis of cloud computing and Fog computing

Parameter/Feature	Cloud Computing	Fog Computing
Latency	Higher latency due to remote data centers	Lower latency with processing closer to the source
Geographical Distribution	Centralized with large data centers	Decentralized, distributed nodes near the edge
Scalability	Highly scalable, but may involve higher costs	Scalable in localized environments, limited by edge resources
Data Processing	Centralized, remote data processing	Distributed, local data processing
Security and Privacy	Centralized security, but data travels over the internet	Enhanced privacy by processing data locally
Energy Consumption	High energy consumption in large data centers	Lower energy consumption with local processing
Bandwidth Usage	High, as data is sent to central servers	Reduced, as only relevant data is transmitted
Real-Time Processing	Not ideal for real-time applications due to latency -	Suitable for real-time processing and low latency applications

It is primarily a collection of hardware and software systems that can monitor, control, and analyze data with very low latency [33]. In addition, long term storage is not provided by fog computing. It cuts expenses and decreases demand by eliminating unnecessary data from cloud compute storage. Fog devices and cloud devices vary slightly in terms of where they reside and the programs that are installed on them [34].

3. THE ARCHITECTURE OF FOG COMPUTING

The architectural framework of fog computing has an extremely popular research area in recent years. Most research in this area refers to a three-layer architecture that combines IoT, fog computing, and cloud computing. By allocating computational resources near to the end users, this strategy not only improves the efficiency of data processing and storage but also tackles the issues of latency and bandwidth. This tiered method provides a dynamic reaction to the increasing need for real-time data analysis and response as the IoT spreads [35] [36] [37]. Moreover, a more comprehensive N-layer reference design [38] has been specified by the OpenFog Consortium and might be seen as an improvement of the three-layer one. An overview of the Fog framework is provided in the following subsection.

3.1 The Three Layer Architecture

Figure 1 shows the basic three layer framework of fog computing. It stems from the primary concept of fog computing, which is a non-trivial Cloud computing extension within the Cloud-to-Things continuum. In fact, it offers a middle layer the fog layer that fills in the space between IoT devices and cloud infrastructure. Below is a description of the three levels that make up the architecture.

A. The Edge/IoT Layer: IoT devices, such as sensors, smart cars, drones, tablets, smartphones, and more, constitute this layer. The main function of these devices, which are usually dispersed over large geographic areas, is to sense data and send it to higher levels for processing or storage. Nonetheless, certain gadgets, such as highly computationally capable smartphones, can also carry out local processing before to elevating jobs to higher levels. By lowering latency and bandwidth usage, this method not only increases efficiency but also improves system responsiveness and allows for real-time data processing closer to the source.

B. The Fog Layer: The Fog computing architecture is supported by this layer, which is composed of up of several Fog nodes. The OpenFog Consortium defines a fog node as "the physical and logical network element that implements fog computing capabilities [38]." Between end-user devices and the Cloud, these nodes can be placed anywhere and have the ability to compute, transmit, and store data temporarily. In order to deliver services, Fog nodes interface with the cloud infrastructure on the one hand and directly connect with end devices on the other. Fog nodes, for instance, can make advantage of cloud resources like processing power and storage while also giving users personalized contextual information. By relocating computing closer to the data source, Fog nodes can improve processing efficiency, lower latency, and allow real-time applications thanks to their dual connectivity, all while preserving a smooth interface with the larger Cloud network. Furthermore, the system fault tolerance and scalability are enhanced by the decentralized nature of Fog nodes.

C. The Cloud Layer The layer is primarily made up of a centralized cloud architecture with high performance dedicated servers that can store a large amount of data and process a wide range of applications. The Fog computing model allows for the effective migration of computations and services from the cloud to Fog layers, in contrast to traditional cloud computing designs. By optimizing the allocation of jobs across the network, this technique reduces the burden on cloud resources and improves overall efficiency. Furthermore, the technique works especially well in situations when decisions need to be made quickly and with minimal latency, such as in IoT applications and smart environments

The OpenFog Consortium N-tier framework [38] is intended to offer a comprehensive framework inside the Fog layer of the three-tier architecture. Stakeholders can use this design as a guide when implementing fog computing in different scenarios. Although Fog systems and software are deployed according to particular use cases, the core elements of the Fog architecture are always present in all Fog deployments. Nodes farther away from end devices have more processing power and computational capacity in the N-tier Fog layer architecture. The Fog layer tiers are designed to handle data extraction and processing at ever higher levels of complexity. Contextual considerations including the number of end devices, the workload that each tier handles, the capabilities of nodes at each level, and latency requirements determine the exact number of

tiers in a deployment. Inter-tier communication also makes it possible to build a mesh network, which promotes improved load balancing, fault tolerance, and resilience. By enabling both vertical and horizontal communication across fog nodes, this design improves the overall robustness and efficiency of the system.

3.2 Key Aspects Of Fog Computing

Fog computing has become a vital component in the rapidly developing field of the IoT, facilitating intelligent and effective data processing. Fog Computing overcomes the drawbacks of traditional cloud computing, including latency, bandwidth restrictions, and security issues, by providing the cloud capabilities closer to the edge of the network. This decentralized method is essential for applications that call for quick replies and localized processing since it enables real-time data analysis and decision-making. Comprehending the fundamentals of fog computing will help us understand how this technology is transforming industries such as healthcare, smart cities, industrial automation, smart grids, autonomous vehicles, smart agriculture, and intelligent traffic management by enabling a more responsive, secure, and scalable computing environment. Fog Computing is at the forefront of driving innovation across varied industries, whether it is improving the efficiency of autonomous vehicles, optimizing energy distribution in smart grids, or enabling real-time decision-making in critical healthcare scenarios [39] [40] [41][42] [43] [44]. Thus, in relation to nearer user network edge devices, fog computing provided a range of functionalities for IoT devices such as computation, processing, interaction, and confinement. The most important and advantageous feature of fog computing, in comparison to other traditional computing models, is the provided service capacity, which demonstrated proximity to IoT devices [45]. The key features and characteristics of fog computing is depicted in Fig. 2.

3.3 Fog Computing Security Issues And Challenges

By processing data nearer to the source, fog computing delivers cloud computing services to the edge of the network with the goal of increasing efficiency and lowering latency. Although there are many advantages to this strategy, it also poses a number of security risks and difficulties which are discussed below and need to be resolved in order to guarantee the confidentiality and integrity of the data.

- Allocating resources and optimization: In fog computing environments, effective strategies and procedures are needed for resource allocation. In order to improve the efficiency and dependability of fog computing systems, future research in this field may concentrate on developing methods for changing resource optimization and allocation [46] [47].

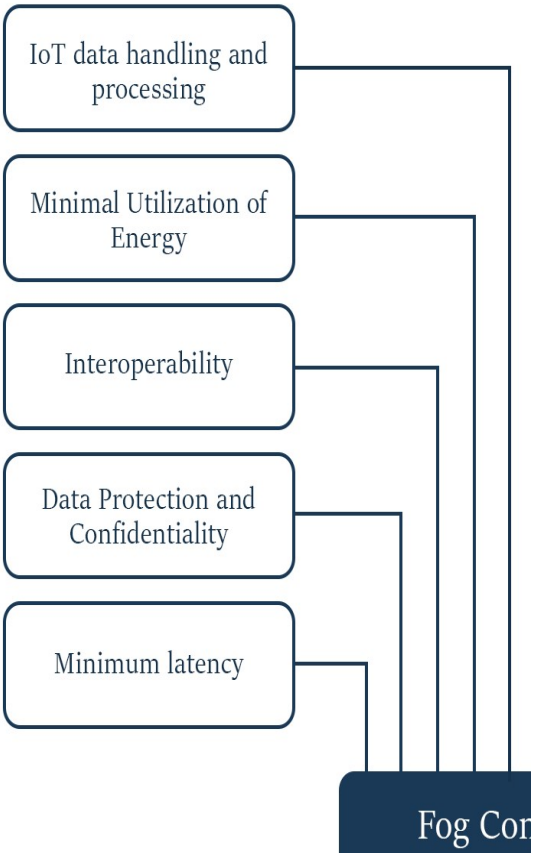

Figure 2: Key Features of Fog Computing

- Security and Privacy: Systems using fog computing are susceptible to many security threats, such as denial-of-service attacks and data breaches, and many others [48].
- Edge device intelligence: Algorithms for artificial intelligence (AI) and machine learning can be applied closer to the data source at the edge of the network by utilizing fog computing. Edge intelligence and analytics research can improve the efficacy and performance of fog computing systems [49].

- Distributed and Real-time applications: The distributed and real-time capabilities of fog computing can be used, for example, in the deployment of IoT and 5G systems. Research in this area may focus on developing methods for distributed, real-time computing in fog environments as well as on identifying novel fog computing use cases and applications [50].
- Augmented Reality (AR) Technology: It is the technology to enhances an individual perception of the external world by overlaying digital data on top of it. Head-mounted displays (HMDs) or smartphones can be utilized for this. Fog computing and augmented reality (AR) have been seen to be increasingly popular in recent years as a way to create more immersive and responsive experiences. Numerous benefits result from combining AR and fog computing, such as real-time processing, low latency, and scalability. This technology has the strength to create more responsive and immersive experiences, especially in the context of smart cities and industrial applications [51]. Enhancing the latency and responsiveness of augmented reality apps and developing new augmented reality use cases that take advantage of fog computing capabilities could be the main goals of research in this area. Intelligent transportation networks, smart cities, and industrial automation are a few examples of these application scenarios. Additionally, when developing and putting into practice fog-based AR systems, security and privacy issues specific to AR should be taken into account.
- Resource management using quantum computing: Demands for data collection and processing have surged as a result of the Internet of Things. Fog computing provides a solution by moving services closer to end devices, but cloud computing suffers from latency because of its centralized architecture. However, because fog computing is distributed and resource-constrained, it presents difficulties for secure resource management. Techniques in quantum computing might offer practical answers to these problems [52]
- Error correction and detection strategies: Error correction techniques are crucial in fog computing because they guarantee data integrity and system dependability throughout dispersed computing layers. Because fog nodes are diverse and dynamic, fog computing environments—which disperse processing closer to the data source—face special difficulties such data inconsistency and transmission problems. Robust error correction techniques can be implemented inside these fog layers to greatly improve system performance and data quality [53].

3.4 Possible Attacks In Fog Computing

The decentralized nature of fog computing leaves the system open to various security flaws and possible intrusions. Fog computing presents different issues due to its heterogeneous and often resource constrained nodes, unlike standard cloud computing where security procedures are centralized. Threats and attacks of numerous types may target these nodes, which comprise a range of edge devices and intermediate fog nodes. some of the attacks can be observed in Fig. 3. The subsequent section explains the specifics of the attacks and threats.

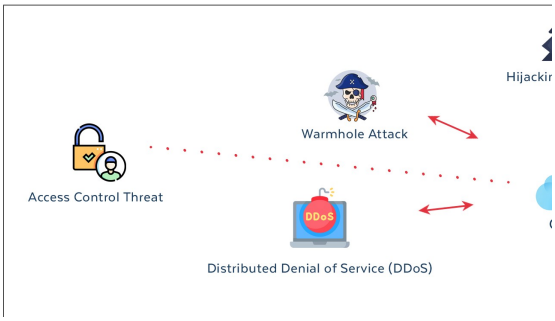

Figure 3: Possible Attacks to the Fog Environment

The Data threats refer to vulnerabilities that impact the data kept on servers and have the ability to exploit user and server information [54]. If unauthorized users obtain access to sensitive data, there may be a breach. This data can be used by these malicious people for their own ends [55]. An organization or business may be impacted by this, and there may be significant losses. Another fog computing network level vulnerability is account hijacking. In this attack, unauthorized and malicious people take control of user accounts in an attempt to steal user data and information for their own evil purposes. Phishing is a strategy used in account hijacking. This issue can be resolved with the aid of user identity management, network monitoring, information leak prevention technologies, and

vulnerability assessment technologies. Another way to prevent this issue is to employ the decoy approach [56]. One of the most frequent concerns regarding data in fog computing is data breaching. This violates the confidentiality of the data. It causes data to leak, and malevolent and unauthorized users are able to access this info. This problem impacts both the providers' and users data. Encrypting the data is the solution to the data breach. Using multifactor authentication is another helpful method to get around this problem. Another method that fog might employ to prevent the problem of data breaches is decoy [56]. Data loss is yet another problem in fog computing. Errors in data storage, data deletion, and data corruption are the main causes of data loss. When a brute force attack against cloud service providers occurred in 2013, over 44% of service providers were compromised. In fog computing, data loss must be avoided by making backups and using data recovery methods. DOS stops authorized users from utilizing the services provided by fog servers. It is accomplished by using up all of a system limited resource. The attack causes a delay between fog services and end users. Because many IoT devices were not mutually validated, the DoS assaults were simply started. The undermined devices can demand infinite fog node processing or storage resources for legal devices to avoid fog service access [57]. IDS may be used to counter this attack [56]. In the context of fog computing, a DDoS attack is a kind of cyber-attack in which numerous hijacked devices often referred to as a botnet—are utilized to overwhelm a fog node or network with excessive data. The attack aims to overload the target system, rendering it inaccessible to authorized users and interfering with regular operations. Use a machine learning-based DDoS defender at the SDN controller to evaluate, forecast, and filter incoming traffic, allowing only valid packets through, in order to counter DDoS attacks in fog and cloud computing [58]. The Man-in-the-Middle Attack (MitM) occurs in fog computing when an attacker eavesdrops in on two nodes within the fog network and may modify their communication. The close proximity of fog nodes to end devices, which leaves them open to interception in the absence of the strong security protections present in centralized cloud data centers, makes this kind of assault especially risky in fog environments. An IPS with lightweight encryption works to protect communication, and an IDS can be used to periodically scan neighboring nodes for compromise in order to prevent MitM attacks in fog computing. This method minimizes latency and energy consumption while providing protection against MitM and associated threats such as packet modification and eavesdropping [59]. The rogue gateway is a malicious entity that exploits the decentralized nature of a fog network to its advantage is known as a rogue gateway. These gateways can conduct attacks like MitM attacks since they are disguising themselves as authentic nodes. They can jeopardize the availability, confidentiality, and integrity of data within the network by intercepting and altering data. This could result in data breaches, unauthorized access, and service interruptions. Furthermore, rogue gateways can enable further attacks like as data tampering, unauthorized data rerouting, and eavesdropping, which poses a serious risk to the fog computing environment overall security. It is imperative to incorporate resilient detection techniques, such encryption and ongoing node verification, in order to reduce the threats that these rogue organizations represent [34]. The Access Control treat problem may lead to inadequate administration. Additionally, anyone not allowed to use fog services can do so. It is possible for any user to install software and modify configuration. MFA must be implemented, strong encryption techniques, and frequent audits must be carried out, in order to effectively address access control concerns in fog computing [56]. The Advance Persistent Threats (APTs) are persistent, focused attacks designed to steal confidential information. Enforce rigorous access rules and encryption on all fog nodes, maintain frequent updates and patches, and deploy strong monitoring with anomaly detection to manage APTs [60] [61]. The Jamming in Fog computing can cause degraded or stopped activities in fog computing settings by overloading communication networks with fake signals or data. Fog nodes are especially susceptible to these kinds of assaults since they frequently rely on wireless communications, which can result in loss of data integrity and service interruption. Adding redundancy and network heterogeneity can improve defenses against assaults using jamming techniques [34]. Eavesdropping, which affects fog environments, is the act of intercepting and examining transmission packets in order to obtain unauthorized access to private information. To avoid unwanted packet interception, adopt robust encryption algorithms for data in transmission [62]. Another serious attack which is a wormhole attack that entails the formation of a tunnel by two or more compromised nodes in order to intercept and reroute data packets, which may result in data loss, manipulation, or interference with network

functions. Use strong routing protocols with node authentication and integrity checks to thwart wormhole attacks. Use encryption to secure data transfer and keep an eye out for irregularities in network traffic to make sure intercepted packets cannot be easily modified or diverted [63]. Similarly a blackhole attack is a hostile fog node poses as a trustworthy node in a blackhole attack, but instead of forwarding packets, it drops them, causing data loss and communication problems. Implement node authentication and verification procedures to make sure that only reliable nodes are a part of the network in order to counteract blackhole attacks. To find and isolate hostile nodes, use routing protocols that have built-in detection for suspicious behavior and routinely examine network traffic for anomalies [64] [65]. Another attack known as a grayhole attack, which is a variation on a blackhole attack, a malicious fog node appears to be appropriately passing data, but fact it drops packets on purpose. Since this kind of attack keeps end-to-end communication, it is difficult to identify. Establish in place reliable routing protocols with checkpoints and validation procedures for packet transfer. To guarantee data integrity, use redundancy in your data channels. You can also use anomaly detection systems to find differences between the packet delivery rates that are reported and the actual rates. Audit network performance on a regular basis to find and remove rogue nodes [66] [59]. Likewise the Sybil attack in fog computing is when a malicious adversary creates several fake nodes in order to interfere with activities or take advantage of resources. Use robust identity verification techniques, put reputation mechanisms in place to keep an eye on node behavior, limit resource access for individual nodes, and enforce secure communication protocols to safeguard the network integrity [67] [68]. The Web Oriented Attacks in Fog Computing focus on security holes in online applications running on edge data centers, including unsafe direct object sources, SQL injection, cross-site scripting (XSS), forging requests, and session or account hijacking. These assaults may result in compromised program functionality and data leaks. Use robust input validation and sanitization to stop SQL injection and XSS attacks that target websites. In order to guard against this use secure authentication methods. To stop unsafe object references, implement appropriate access constraints. Update and patch software frequently to address security flaws, and install web application firewalls (WAFs) to identify and stop malicious activity. To find and eliminate any threats, do routine penetration tests and security audits [35] [69]. The attacks Based on Malware in Fog Computing: Trojan horses, worms, ransomware, and spyware are examples of malware that can compromise node security and interfere with fog computing operations. It is critical to utilize network segmentation, implement sophisticated anti-malware solutions, update software often, impose stringent access rules, and periodically backup important data in order to combat these threats. Furthermore, deploying IDS and educating users can aid in the efficient detection and mitigation of malware attacks [70] [71]. Further research should investigate the incorporation of quantum cryptography methods to improve the security and secrecy of data transmission between fog nodes and edge devices. Employing the ideas of quantum mechanics, quantum cryptography ensures that data cannot be intercepted or altered by malevolent parties by offering unbreakable encryption [72]. In fog computing environments, where sensitive data is frequently transmitted between devices that may be geographically scattered and prone to attacks, this is particularly important. Quantum cryptography can be incorporated with fog computing systems to create safe communication channels that can withstand even the most advanced hacking methods. This would safeguard sensitive data privacy and significantly enhance the general security of fog computing networks. Quantum key distribution can be one of the solutions.

3.5 Synergy Between Fog Computing And Iot

The integration of fog computing and the IoT produces a strong and beneficial ecosystem that improves the responsiveness, scalability, and efficiency of contemporary computing systems. The IoT creates massive amounts of data at the network edge due to its extensive network of linked devices. Processing this data in real-time is frequently necessary, which is where fog computing comes in handy. Fog Computing lessens the latency and bandwidth requirements that might otherwise strain centralized cloud systems by processing and analyzing data closer to its source. Furthermore, Fog Computing distributed architecture blends in seamlessly with the IoT decentralized design. Fog nodes can be placed deliberately to manage limited data processing tasks, whereas IoT devices are usually distributed over large geographic areas. By dispersing processing capacity, this method not only increases the scalability but also the durability of IoT networks. The architecture facilitates a more intelligent and adaptable computing environment by

integration of Fog Computing with IoT environment. IoT sensors, for instance, can track a patient vital sign in real time in smart healthcare, and adjacent Fog nodes can process this data quickly to send out alerts right away if there are any irregularities. Likewise, Fog Computing can assist in managing the huge amounts of data produced by sensors throughout the network in smart grids, maximizing energy distribution and guaranteeing stability. Similarly, IoT-enabled field data is gathered by weather stations and soil moisture sensors, among other IoT devices, and processed by Fog nodes to deliver real-time insights and automatic irrigation system control. This guarantees maximum crop yield, ideal growing conditions, and economical use of water. The local data processing capabilities of fog computing are especially useful in isolated agricultural regions with spotty or nonexistent access to centralized cloud servers. Likewise, IoT-enabled automobiles and traffic sensors produce constant streams of data for smart traffic management. Real-time data analysis by fog nodes at junctions and along roadways can optimize traffic light timing, lessen congestion, and enhance safety. For applications where prompt decision-making is crucial, such as autonomous driving, this concentrated processing minimizes latency. In a comparable manner, IoT devices in smart factories track production lines, keep an eye on machinery, and provide quality control. By processing this data locally, fog nodes enable real-time modifications to production procedures and reduce downtime. By supporting predictive maintenance and increasing operational efficiency, this localized computing lowers costs and boosts output. Six distinct uses of fog computing in conjunction with the IoT are shown in Figure 4. This illustration demonstrates how real time analytics and localized data processing offered by fog computing with IoT environment improve a number of industries, including smart manufacturing, smart grids, smart healthcare, smart agriculture, and smart traffic management.

3.5.1 Challenges And Issues To The Fog Computing And Iot Ecosystem

There are many challenges and limitations with integrating fog computing in Internet of Things systems. Issues about privacy and security are substantial. The security of Internet of Things devices is a major concern that involves both digital and physical vulnerabilities. Secure low-power network connectivity and the requirement for lightweight authentication methods are important concerns [73] [74]. The security of the systems in the real scenarios is another crucial component of IoT security. In the world of the digital world, there are now serious concerns due to the enormous rise in Distributed Denial of Service (DDoS) assaults in the IoT era [75].

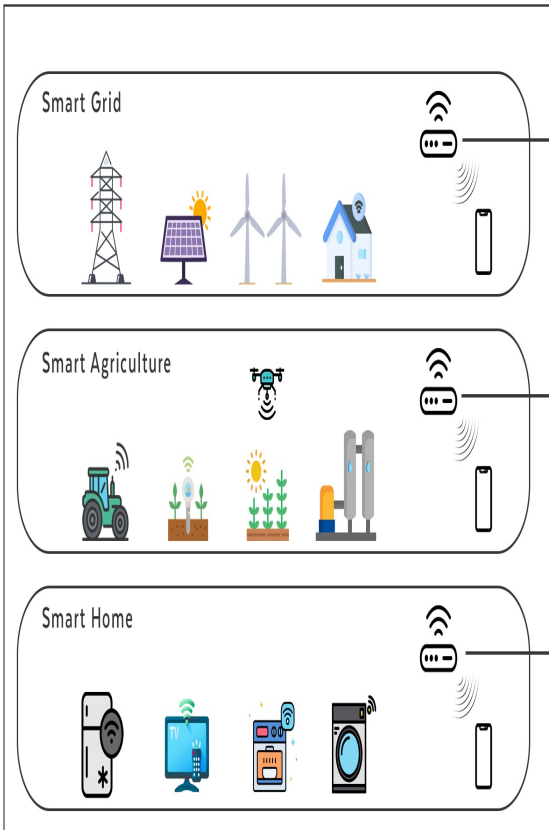

Figure 4: A Scenario Of Six Different Uses For Fog Computing In Combination With The Internet Of Things

Furthermore, there are limitations on the security features that may be added to smart devices due to resource limitations. This raises important questions about the IoT environment and encourages further study into lightweight safety measures [74]. IoT networks have special characteristics that make IoT forensics quite challenging. The large number of linked devices makes gathering data, analysis, and preservation highly challenging. This is especially true in IoT contexts, which are dynamic and heterogeneous. These difficulties are made worse by elements including data instability, device storage limitations, and the possibility of cross-border concerns [76]. In relation to this, privacy is important and affects IoT devices that people may engage with directly. When gathering user privacy-related data, for example, this kind of device faces particular difficulties. An open problem is to conduct research into privacy models that can

handle the complexity of figuring out which devices in an IoT network have access to privacy-sensitive data and should have that access [77]. Because fog computing involves a wide variety of devices and protocols, interoperability problems can occur. Effective integration and communication between different Fog nodes and IoT devices may be hampered by a lack of standards. In order to facilitate the smooth integration of various devices and systems, interoperability is essential to the IoT ecosystem. It guarantees that many parts can cooperate effectively, which is particularly crucial in intricate settings like smart cities etc. IoT applications that deal with issues or demand fast reactions, in particular, may become ineffective and inefficient due to a lack of compatibility. The research conducted by the authors emphasizes how critical it is to solve interoperability issues in IoT. They offer a thorough analysis of current approaches, classifying them according to situations and domains. Although there are existing responses, their investigation indicates that a more comprehensive strategy is required. In order to achieve this, they provide a hybrid framework that is intended to improve IoT interoperability, providing a dependable and all-encompassing solution, especially for smart cities [78].

Because fog nodes are spread, there is a greater attack surface, so it is essential to apply the same security procedures to every node [79]. As data is handled locally, there is an increasing complexity in ensuring data privacy and regulatory compliance. Scalability is another difficulty; it takes careful planning and infrastructure investment to manage resources among multiple Fog nodes while balancing loads and handling growing network traffic [80]. The task of managing limited local storage capacity and ensuring data consistency and synchronization across dispersed nodes adds to the complexity of the situation. Despite Fog Computing advantage of lowering latency by processing data closer to the source, performance and latency remain major challenges. Persistent problems include preventing resource bottlenecks and guaranteeing optimal performance across distant nodes. Due to its complexity and resource requirements, deployment and maintenance need for efficient distributed infrastructure management and monitoring [81]. Energy consumption is still an issue since distributed nodes power needs must be managed, especially in remote or mobile situations. Furthermore, setting up and maintaining a Fog Computing infrastructure can be expensive due to the significant startup costs as well as continuous operating costs [78]. The integration process is further complicated by difficulties related to regulatory compliance and data sovereignty, as it can be difficult to guarantee compliance with data protection rules in many jurisdictions. Lastly, in order to assure compatibility, integrating fog computing with current legacy systems frequently necessitates substantial alterations and careful design. A comprehensive approach including strong security protocols, effective resource management, and meticulous deployment planning is necessary to meet these problems [76].

4. CONCLUSION AND FUTURE DIRECTIONS

The IoT and fog computing integration offer major potential to improve the efficiency, scalability, and responsiveness of modern IT infrastructures. Fog computing decentralized structure, however, presents special security risks and possible threats. Data threats, account hijacking, DoS attacks, MitM attacks, rogue gateways, access control problems, APTs, jamming, eavesdropping, wormhole attacks, blackhole attacks, Sybil attacks, and web-oriented attacks are only a few of the challenges that have been thoroughly covered in the present article. The paper additionally discusses the unique security challenges that fog computing faces, including resource limitations, heterogeneous nodes, security and privacy issues, vulnerabilities in IoT devices, forensics difficulties, interoperability issues, scalability constraints, performance and latency issues, energy consumption, regulatory compliance, and challenges integrating legacy systems. Ensuring the effective implementation of fog computing in Internet of Things environments will require addressing the issues outlined in this study. Subsequent investigations ought to concentrate on developing strong security procedures and protections against different kinds of assaults and decreasing the weaknesses of fog computing systems. It is also critical to look into low-power security options appropriate for fog nodes and IoT devices with limited resources. Another crucial area of research is the investigation of novel strategies for IoT forensics that address the challenges associated with data gathering, processing, and preservation in dynamic and heterogeneous fog computing. For seamless integration and communication, it is essential to address interoperability challenges by encouraging standardization and creating suitable protocols and frameworks for fog computing and IoT devices. To maximize the performance and use of fog computing resources, it is also crucial to look at scalable and effective resource management

techniques. Another crucial factor to take into account is the development of energy-efficient solutions that reduce fog node power consumption and increase their sustainability. It is also critical to address confidentiality and regulatory compliance issues to make sure fog computing systems comply by applicable laws and regulations. Exploring methods to employ quantum cryptography to protect the links that fog nodes and edge devices have for communication. Encryption using quantum cryptography methods can be unbreakable, guaranteeing the integrity and confidentiality of data sent through these avenues. Applications like healthcare, finance services, and many other latency acute applications that need to transmit extremely sensitive data can discover this to be particularly useful.

subsequently, research into fog computing integration with cutting-edge technologies like blockchain, AI, and machine learning, quantum communication can expand its applications and address novel challenges. The full potential of fog computing in IoT environments can be realized by addressing these issues and investigating future research avenues, which will result in more scalable, secure, and effective solutions for a range of applications.

REFERENCES

[1] V. Friedman, "On the edge: Solving the challenges of edge computing in the era of iot," URL: https://data-economy. com/on-the-edge-solving-the-challenges-of-edge-computing-in-theeraof-iot, 2018.

[2] F. Hosseinpour, P. Vahdani Amoli, J. Plosila, T. H¨am¨al¨ainen, and H. Tenhunen, "An intrusion detection system for fog computing and iot based logistic systems using a smart data approach," International Journal of Digital Content Technology and its Applications, vol. 10, no. 5, 2016.

[3] B. Cao, Y. Zhang, J. Zhao, X. Liu, L. Skonieczny, and Z. Lv, "Recommendation based on large-scale many-objective optimization for the intelligent internet of things system," IEEE Internet of Things Journal, vol. 9, no. 16, 2021, pp. 15 030–15 038.

[4] V. Chang, L. Golightly, P. Modesti, Q. A. Xu, L. M. T. Doan, K. Hall, S. Boddu, and A. Kobusi´nska, "A survey on intrusion detection systems for fog and cloud computing," Future Internet, vol. 14, no. 3, 2022, p. 89.

[5] H. Akbar, M. Zubair, and M. S. Malik, "The security issues and challenges in cloud computing," International Journal for Electronic Crime Investigation, vol. 7, no. 1, pp. 13–32, 2023.

[6] N. Peter, "Fog computing and its real time applications," Int. J. Emerg. Technol. Adv. Eng, vol. 5, no. 6, 2015, pp. 266–269.

[7] C. Bhatt and C. Bhensdadia, "Fog computing: Applications, concepts, and issues," International Journal of Grid and High Performance Computing (IJGHPC), vol. 9, no. 4, pp. 105–113, 2017.

[8] O. A. Alzubi, J. A. Alzubi, M. Alazab, A. Alrabea, A. Awajan, and I. Qiqieh, "Optimized machine learning-based intrusion detection system for fog and edge computing environment," Electronics, vol. 11, no. 19, p. 3007, 2022.

[9] L. Yi, M. Yin, and M. Darbandi, "A deep and systematic review of the intrusion detection systems in the fog environment," Transactions on Emerging Telecommunications Technologies, vol. 34, no. 1, p. e4632, 2023.

[10] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," Future Generation Computer Systems, vol. 78, pp. 680–698, 2018. [11] H. A. Afolabi and A. Aburas, "Proposed back propagation deep neural network for intrusion detection in internet of things fog computing," Int J, vol. 9, no. 4, pp. 464–469, 2021.

[12] M. A. Aladaileh, M. Anbar, I. H. Hasbullah, Y.-W. Chong, and Y. K. Sanjalawe, "Detection techniques of distributed denial of service attacks on software-defined networking controller–a review," IEEE Access, vol. 8, pp. 143 985–143 995, 2020.

[13] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A systematic literature review on cloud computing security: threats and mitigation strategies," Ieee Access, vol. 9, pp. 57 792–57 807, 2021.

[14] I. Stojmenovic and S. Wen, "The fog computing paradigm: Scenarios and security issues," in 2014 federated conference on computer science and information systems. IEEE, 2014, pp. 1–8.

[15] H. R. Abdulqadir, S. R. Zeebaree, H. M. Shukur, M. M. Sadeeq, B. W. Salim, A. A. Salih, and S. F. Kak, "A study of moving from cloud computing to fog computing," Qubahan Academic Journal, vol. 1, no. 2, pp. 60–70, 2021.

[16] S. A. Bello, L. O. Oyedele, O. O. Akinade, M. Bilal, J. M. D. Delgado, L. A. Akanbi, A. O. Ajayi, and H. A. Owolabi, "Cloud computing in construction industry: Use cases, benefits and challenges," Automation in Construction, vol. 122, p. 103441, 2021.

[17] W. Shi and S. Dustdar, "The promise of edge computing," Computer, vol. 49, no. 5, pp. 78–81, 2016.

[18] K. Dolui and S. K. Datta, "Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing," in 2017 Global Internet of Things Summit (GIoTS). IEEE, 2017, pp. 1–6.

[19] O. Jouini, K. Sethom, A. Namoun, N. Aljohani, M. H. Alanazi, and M. N. Alanazi, "A survey of machine learning in edge computing: Techniques, frameworks, applications, issues, and research directions," Technologies, vol. 12, no. 6, p. 81, 2024.

[20] H. Nouhas, A. Belangour, and M. Nassar, "Cloud and edge computing architectures: A survey," in 2023 IEEE 11th Conference on Systems, Process & Control (ICSPC). IEEE, 2023, pp. 210–215.

[21] O. Consortium et al., "Glossary of terms related to fog computing," Accessed: Jul, vol. 10, p. 2018, 2018.

[22] H. Pang and K.-L. Tan, "Authenticating query results in edge computing," in Proceedings. 20th International Conference on Data Engineering. IEEE, 2004, pp. 560–571.

[23] R. Grieco, D. Malandrino, and V. Scarano, "Secs: scalable edge-computing services," in Proceedings of the 2005 ACM symposium on Applied computing, 2005, pp. 1709–1713.

[24] G. P. Center, "A simple report on cybersecurity,"https://www.google.com/press/podium/ses2006. html, 2018, accessed: 2024-07-10.

[25] B. Hayes, "Cloud computing," 2008.

[26] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities," in 2008 10th IEEE international conference on high performance computing and communications. Ieee, 2008, pp. 5–13.

[27] R. A. Dolin, "Deploying the" internet of things"," in International Symposium on Applications and the Internet (SAINT'06). IEEE, 2006, pp. 4–pp.

[28] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in Proceedings of the first edition of the MCC workshop on Mobile cloud computing, 2012, pp. 13–16.

[29] E. Badidi and A. Ragmani, "An architecture for qos-aware fog service provisioning," Procedia Computer Science, vol. 170, pp. 411–418, 2020.

[30] A. Mebrek, L. Merghem-Boulahia, and M. Esseghir, "Efficient green solution for a balanced energy consumption and delay in the iot-fog-cloud computing," in 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA). IEEE, 2017, pp. 1–4.

[31] N. Dahiya, S. Dalal, and V. Jaglan, "Efficient green solution for a balanced energy consumption and delay in the iot-fog-cloud computing," in Green Internet of Things for Smart Cities. CRC Press, 2021, pp. 113–123.

[32] V. Marbukh, "Towards fog network utility maximization (fonum) for managing fog computing resources," in 2019 IEEE International Conference on Fog Computing (ICFC). IEEE, 2019, pp. 195–200.

[33] R. R. Ema, T. Islam, and M. H. Ahmed, "Suitability of using fog computing alongside cloud computing," in 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE, 2019, pp. 1–4.

[34] A. M. Alwakeel, "An overview of fog computing and edge computing security and privacy issues," Sensors, vol. 21, no. 24, p. 8226, 2021.

[35] I. Kabashkin, "End-to-end service availability in heterogeneous multi-tier cloud–fog–edge networks," Future Internet, vol. 15, no. 10, p. 329, 2023.

[36] N. Ghani, A. A. B. Sajak, R. Qureshi, M. F. A. Zuhairi, and Z. M. P. A. Baidowi, "A review of fog computing concept, architecture, application, parameters and challenges," JOIV: International Journal on Informatics Visualization, vol. 8, no. 2, pp. 564–575, 2024.

[37] P. Habibi, M. Farhoudi, S. Kazemian, S. Khorsandi, and A. Leon-Garcia, "Fog computing: a comprehensive architectural survey," IEEE access, vol. 8, pp. 69 105–69 133, 2020.

[38] A. OpenFog Consortium Architecture Working Group et al., "Openfog reference architecture for fog computing," OPFRA001, vol. 20817, p. 162, 2017.

[39] M. M. Hussain and M. S. Beg, "Fog computing for internet of things (iot)-aided smart grid

architectures," Big Data and cognitive computing, vol. 3, no. 1, p. 8, 2019.

[40] V. K. Quy, N. V. Hau, D. V. Anh, and L. A. Ngoc, "Smart healthcare iot applications based on fog computing: architecture, applications and challenges," Complex & Intelligent Systems, vol. 8, no. 5, pp. 3805–3815, 2022.

[41] E. Guardo, A. Di Stefano, A. La Corte, M. Sapienza, and M. Scat`a, "A fog computing-based iot framework for precision agriculture," Journal of Internet Technology, vol. 19, no. 5, pp. 1401–1411, 2018.

[42] M. K. Saroa and R. Aron, "Fog computing and its role in development of smart applications," in 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCo m). IEEE, 2018, pp. 1120–1127.

[43] K. V. R. Kumar, K. D. Kumar, R. K. Poluru, S. M. Basha, and M. P. K. Reddy, "Internet of things and fog computing applications in intelligent transportation systems," in Architecture and security issues in fog computing applications. IGI Global, 2020, pp. 131–150.

[44] K. Behravan, N. Farzaneh, M. Jahanshahi, and S. A. H. Seno, "A comprehensive survey on using fog computing in vehicular networks," Vehicular Communications, vol. 42, p. 100604, 2023.

[45] M. Chiang and T. Zhang, "Fog and iot: An overview of research opportunities," IEEE Internet of things journal, vol. 3, no. 6, pp. 854–864, 2016.

[46] G. S. Rahman, T. Dang, and M. Ahmed, "Deep reinforcement learning based computation offloading and resource allocation for low-latency fog radio access networks," Intelligent and Converged Networks, vol. 1, no. 3, pp. 243–257, 2020.

[47] B. Jia, H. Hu, Y. Zeng, T. Xu, and Y. Yang, "Double-matching resource allocation strategy in fog computing networks based on cost efficiency," Journal of Communications and Networks, vol. 20, no. 3, pp. 237–246, 2018.

[48] G. Sun, S. Sun, J. Sun, H. Yu, X. Du, and M. Guizani, "Security and privacy preservation in fogbased crowd sensing on the internet of vehicles," Journal of Network and Computer Applications, vol. 134, pp. 89–99, 2019.

[49] T. Zhang, Z. Shen, J. Jin, X. Zheng, A. Tagami, and X. Cao, "Achieving democracy in edge intelligence: A fog-based collaborative learning scheme," IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2751–2761, 2020.

[50] E. Gomes, F. Costa, C. De Rolt, P. Plentz, and M. Dantas, "A survey from real-time to near realtime applications in fog computing environments," in Telecom, vol. 2, no. 4. MDPI, 2021, pp. 489–517.

[51] S. M. Salman, T. A. Sitompul, A. V. Papadopoulos, and T. Nolte, "Fog computing for augmented reality: Trends, challenges and opportunities," in 2020 IEEE International Conference on Fog Computing (ICFC). IEEE, 2020, pp. 56–63.

[52] T. Veni, "Quantum-based resource management approaches in fog computing environments: A comprehensive review," Mobile Computing and Sustainable Informatics: Proceedings of ICMCSI 2022, pp. 743–752, 2022. [53] K. Matsui and H. Nishi, "Error correction method considering fog and edge computing environment," in 2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS). IEEE, 2019, pp. 517–521.

[54] S. Sridhar, R. Sathishkumar, and G. F. Sudha, "Adaptive halftoned visual cryptography with improved quality and security," Multimedia Tools and Applications, vol. 76, pp. 815–834, 2017.

[55] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: Security and privacy issues," IEEE Internet Computing, vol. 21, no. 2, pp. 34–42, 2017.

[56] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: a review of current applications and security solutions," Journal of Cloud Computing, vol. 6, pp. 1–22, 2017.

[57] F. A. Zwayed, M. Anbar, Y. Sanjalawe, and S. Manickam, "Intrusion detection systems in fog computing–a review," in Advances in Cyber Security: Third International Conference, ACeS 2021, Penang, Malaysia, August 24–25, 2021, Revised Selected Papers 3. Springer, 2021, pp. 481–504.

[58] R. Priyadarshini, R. Kumar Barik, and H. Dubey, "Fog-sdn: A light mitigation scheme for ddos attack in fog computing framework," International Journal of Communication Systems, vol. 33, no. 9, p. e4389, 2020.

[59] F. Aliyu, T. Sheltami, and E. M. Shakshuki, "A detection and prevention technique for man in the middle attack in fog computing," Procedia computer science, vol. 141, pp. 24–31, 2018.

[60] S. Feng, Z. Xiong, D. Niyato, and P. Wang, "Dynamic resource management to defend against advanced persistent threats in fog computing: A game theoretic approach," IEEE Transactions on Cloud Computing, vol. 9, no. 3, pp. 995–1007, 2019.

[61] T. Jabar and M. Mahinderjit Singh, "Exploration of mobile device behavior for mitigating advanced persistent threats (apt): a systematic literature review and conceptual framework," Sensors, vol. 22, no. 13, p. 4662, 2022.

[62] Z. Ashi, M. Al-Fawa'reh, and M. Al-Fayoumi, "Fog computing: security challenges and countermeasures," Int. J. Comput. Appl, vol. 175, no. 15, pp. 30–36, 2020.

[63] S. Prabavathy, K. Sundarakantham, and S. M. Shalinie, "Design of cognitive fog computing for intrusion detection in internet of things," Journal of Communications and Networks, vol. 20, no. 3, pp. 291–298, 2018.

[64] S. K. Erskine and K. M. Elleithy, "Real-time detection of dos attacks in ieee 802.11 p using fog computing for a secure intelligent vehicular network," Electronics, vol. 8, no. 7, p. 776, 2019.

[65] A. K. Jumani, J. Shi, A. A. Laghari, Z. Hu, A. u. Nabi, and H. Qian, "Fog computing security: A review," Security and Privacy, vol. 6, no. 6, p. e313, 2023.

[66] A. P. Abidoye, I. C. Obagbuwa, and N. A. Azeez, "Mitigating denial of service attacks in fog-based wireless sensor networks using machine learning techniques," Journal of Data, Information and Management, vol. 5, no. 4, pp. 207–225, 2023.

[67] A. Borah and A. Paranjothi, "Sybil attack detection in vanets using fog computing and beamforming," in 2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). IEEE, 2023, pp. 0626–0631.

[68] A. A. Almazroi, M. H. Alkinani, M. A. Al-Shareeda, M. A. Alqarni, A. A. Almazroey, and T. Gaber, "Fc-lsr: Fog computing-based lightweight sybil resistant scheme in 5g-enabled vehicular networks," IEEE Access, 2024.

[69] S. Mostafavi and W. Shafik, "Fog computing architectures, privacy and security solutions," Journal of Communications Technology, Electronics and Computer Science, vol. 24, pp. 1–14, 2019.

[70] A. A. Alli, K. Kassim, N. Mutwalibi, H. Hamid, and L. Ibrahim, "Secure fog-cloud of things: architectures, opportunities and challenges," Secure edge computing, pp. 3–20, 2021.

[71] A. K. Alhwaitat, S. Manaseer, and R. M. Al-Sayyed, "A survey of digital forensic methods under advanced persistent threat in fog computing environment," Journal of Theoretical and Applied Information Technology, vol. 97, no. 18, pp. 4934–4954, 2019.

[72] M. M. Khan, I. Bari, O. Khan, N. Ullah, M. Mondin, and F. Daneshgaran, "Soft decoding of short/medium length codes using ordered statistics for quantum key distribution," International Journal of Quantum Information, vol. 19, no. 06, p. 2150025, 2021.

[73] Z. Abbas and W. Yoon, "A survey on energy conserving mechanisms for the internet of things: Wireless networking aspects," Sensors, vol. 15, no. 10, pp. 24 818–24 847, 2015.

[74] V. Adat and B. B. Gupta, "Security in internet of things: issues, challenges, taxonomy, and architecture," Telecommunication Systems, vol. 67, pp. 423–441, 2018.

[75] K. Sonar and H. Upadhyay, "A survey: Ddos attack on internet of things," International Journal of Engineering Research and Development, vol. 10, no. 11, pp. 58–63, 2014.

[76] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the internet of things (iot) forensics: challenges, approaches, and open issues," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1191–1221, 2020.

[77] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of things security and forensics: Challenges and opportunities," pp. 544–546, 2018.

[78] S. S. Albouq, A. A. Abi Sen, N. Almashf, M. Yamin, A. Alshanqiti, and N. M. Bahbouh, "A survey of interoperability challenges and solutions for dealing with them in iot environment," IEEE Access, vol. 10, pp. 36 416–36 428, 2022.

[79] R. Qureshi, M. Asad, S. Tunio, S. Qureshi, M. Ahmed, and A. Ghulam, "A survey on security issues and attacks of fog computing," VFAST Transactions on Software Engineering, vol. 11, no. 1, pp. 1–11, 2023.

[80] S. N. Srirama, "A decade of research in fog computing: relevance, challenges, and future directions," Software: Practice and Experience, vol. 54, no. 1, pp. 3–23, 2024.

[81] H. G. Abreha, C. J. Bernardos, A. D. L. Oliva, L. Cominardi, and A. Azcorra, "Monitoring in fog computing: state-of-the-art and research challenges," International Journal of Ad Hoc and Ubiquitous Computing, vol. 36, no. 2, pp. 114–130, 2021.