Survey Paper on Fog Computing and its Security Issues

Abstract

The development of the Internet of Things (IoT) and current trends that require more frequent and almost continuous data processing have called into question the possibilities of using conventional cloud computing systems, including latency and bandwidth issues. Fog computing, an extended version of cloud computing, is increasingly considered an effective solution as computation is de-centralized and made closer to the source. This survey paper aims at presenting a general understanding of the Fog computing that focuses on its architectural model and various aspects of its attributes and application areas for various domains including smart grid, intelligent transportation system including healthcare, and manufacturing IoT. Nevertheless, the introduction of Fog computing comes with new security threats as follows, Device weaknesses, data privacy and integrity, and large attack surface due to the extension of the computing environment. This paper also investigates some of the measures which have been put in place to combine the above-mentioned security threats which include authentication, the use of data encryption, and intrusion detection systems. Finally, it provides direction for future study where AI, and other advanced technologies can be implemented in Fog system for more secure support of real time application needs. This paper has the objective of present a control and deep analysis of Fog computing advantages and security threats, and the measures to avoid them and deploy Fog computing in a safe and massive manner in the future IoT scenarios.

Keywords Fog computing · Internet of Things (IoT) · Real-time data processing · Security challenges · Distributed systems · Data privacy

1 Introduction

1.1 Context and Background

Today's high growth of IoT devices and the need for real time analytic of processed data has put pressure on the traditional Cloud Computing model. Cloud computing which is evident to offer the best solution on how to store, manage and process large data is for most essential based on a centralize architecture[1][6]. This is means the information from the devices or users must be transport across the internet to the cloud data centers; this is causing high latencies, limited bandwidths, and often inadequate scalability; in some cases, for applications that require near real-time data processing and decision making.

Real-time applications can suffer significantly from the latency inherent in cloud computing because of the geographical distance between the source of data and the cloud server. For example, applications in healthcare, industrial automation, or smart grids, demand fast reaction and prompt data processing times. This is especially the case in such scenarios because the back end cloud computing infrastructure essentially cannot provide the level of immediacy needed by these key assets.

This has birthed Fog Computing, a new distributed computing model aimed at bringing computation closer to the data source. As such, Fog computing, by analyzing data at the "edge" of the network closer to where this data is produced, eliminates many of the problems linked to the cloud models. This architecture enables processing data faster and efficiently for real-time applications, instead of waiting for servers from the cloud data centers, they can employ routers, gateway, and edge devices.

Unlike cloud computing scheme which centralised, fog computing is distributed, implemented and spread throughout numerous connected devices and nodes. These devices can aggregate signal information and process it locally; they also have their memory that helps to avoid working with data located on far cloud servers that takes time. In real-time applications such as health monitoring systems or Industrial IoT systems[7], it is eminent to reduce this delay to generate decisions, trigger action, or even real-time alarm. Also, the local processing of data made it easier to address some of such issues as bandwidth since only necessary data to the cloud or summary of the data may be required in some instances.

Nonetheless, the Fog computing topology, unlike the client-server network, has its own vulnerabilities particularly in the area of security[2]. The decentralization inherently present in this model brings new risks, including attack on edge devices, problems with secure communication between them, and barriers to data privacy with a decentralized structure. The technological structure of the network where many ordinary devices having dissimilar levels of computational and security arrangements as compared to the more calibrated Smart devices also pose a challenge in implementing similar security standards into the interconnected system.

That is why with the invention of Fog computing, potential threats such as data leakage, DoS attacks, and others, are possible for a malicious person to become involved in as well. A relatively unique threat to fog computing systems is physical attack since fog computing systems have a close nexus with IoT devices whereby physical tampering with the IoT devices puts on edge nodes at risk of having their hardware and software components compromised. Hence, the challenges experienced in addressing security concerns in Fog computing cannot be solved in isolation of device level security, data encryption, access control and even network security.

Since Faced with the increasing popularity of Fog computing as the successor to conventional cloud models, it is crucial to looking at possible solutions to work against these security threats. This calls for enhanced knowledge on the particular security threats that emerge in Fog systems and research being conducted in their protection of this emerging model.

1.2 Objectives of the Paper

The purpose of this paper is to give the reader an overview of Fog computing with the focus on the principles on which it relies, its components, architecture, and potential uses. In the following sections, we will look at the various levels of fog computing: edge layer, fog nodes, and cloud interface that work in harmony to make distributed processing at the network periphery possible. Furthermore, this paper will outline some of the most pressing security issues related to Fog computing, and more specifically, in relation to IoT use and real-time analytics.

The primary objectives of this survey paper are as follows:

1. **Understanding Fog Computing:** In this paper we will discuss what Fog computing is all about, how it works, how it can expand cloud computing functions. This paper will compare Fog to cloud computing and map out the opportunities and risks of employing Fog computing to various applications.
2. **Identifying Security Issues:** The objective of this research study will therefore be to establish the following: These are the issues to do with the device security, data security, privacy, identity and network security. An additional challenge that fog systems encounter is the relative openness of the architecture of the system, which makes it quite vulnerable to cyber threats such as unauthorized access or attempts to alter the data stored in the network, or even invasion of privacy[8].
3. **Assessing Existing Research:** In order to evaluate existing research efforts to protect Fog computing environments. In this paper, a number of security protocols, frameworks, and models that have being suggested to solve these challenges will be discussed. More specifically, the research will address approaches to protect Edge devices, to preserve the data integrity and confidentiality, and to guarantee safe communication between the Fog nodes and cloud.
4. **Exploring Future Developments:** To present a number of potential future trends and enhancements in Fog computing specifically with regard to addressing scalability, security as well as efficiency issues in the context of the Fog architecture. Potential of incorporating novel technologies including artificial intelligence into Fog systems will also form part of

the topics of the paper. Further, based on our analysis, we will discuss about how the future prospects of Fog computing can be influenced by growing requirement for new applications in real-time .

5. **Examining Applications and Use Cases:** To discuss the various scenarios of the implementation of Fog computing starting from Big Smart Cities, industries, healthcare automation, and the future autonomous systems. The paper will also investigate how implementation of the Fog computing meets the challenge of the sectors and enables ordinary and real-time analysis of big data[9].

2 Overview of Fog Computing

2.1 What is Fog Computing?

Fog computing can be referred to as an architecture model that hinges on cloud computing while intervening it with compute, storage, and services which are as a rule positioned closer to the edge of a network. This paradigm was proposed in order to attend to the increasing complexity of applications and services that depend on online data processing and minimal response time. The traditional concept of cloud computing involves a distributed organization of services whereby all data is processed, stored, and analyzed from a cloud data center after being transferred from end-user devices. However, this model of distribution brings large delays (latency) caused by large distances that data has to travel from a device to a data center and vice versa. Also, with a constant exchange of large data sets between devices and the cloud, such matters as bandwidth issues and general poor utilization of network resources become familiar problems [10].

To overcome these problems, fog computing extends computations and storage closer to the point of origin of data that is often IoT devices, sensors or other edge nodes. In other words, in place of bringing computation to the cloud, Fog computing bring computation closer to the data it has to process, and keeps the data processing on small intermediate nodes in the network known as the Fog nodes. These nodes are often deployed in various areas of the network; for instance, gateways, routers or at some instances, specially developed devices referred to as Fog nodes. These Fog nodes provide computational, storage and networking elements allowing the nodes to perform analytics at the edge and transmit only the necessary information to the cloud.

This Fog node is essential in that it receives and forwards information between IoT devices and cloud layers, carries out the basic functions of data selection, merging, and analysis at the edge of the network. This local processing also keep the amount of raw data to be transported to the cloud to a minimum which make the network to be more efficient. Fog computing, in getting the data closer to the source of origin, helps in cutting on time required to analyze and respond to that data. This leads to low latency, a factor vital for applications that need immediate action like industrial automation, and healthcare[11].

The primary gain that Fog computing makes over cloud computing is reducing latency since data does not have to travel as far. In many technologies, including telecare and smart micro-grid on which the present invention is based, it takes a relatively long time to transfer data from a source to a centralized data center. Fog computing therefore pushes computation to the edge of network so that more critical decisions can be made on time and with less delay.

Also, due to computation at the Fog nodes, Fog computing will also promote bandwidth utilization at the same time. Contrary to what could be achieved in other systems where large data sets are sent to the cloud for processing, only certain subsets of the data or data in aggregate form is transmitted across the network and hence puts less pressure on the actual network. This enhanced data flow helps avoid congestion in a number of available network resources, and is

especially useful in the systems where the network is utilized by a large number of IoT devices, or where the connectivity is constrained or intermittent [12].

Fog computing was introduced by Cisco as an innovative solution to the question of how to manage excessive data generated by IoT devices and process it in time. Cisco always defined fog computing as one of the most promising approaches to address present and future needs for low latency, high bandwidth, and location awareness. The term “Fog” was used to imply that this model straddles the cloud and the devices, in the same way that fog is found between the earth and the sky— at a middle level[36].

Although fog computing is still relatively new and undefined, it is considered to be a successful strategy to support the need of current applications which need both local computation and connection to far away servers. For that reason, Fog computing has high potential in the areas that require near real-time data processing, including smart cities, industrial IoT systems in manufacturing, health care, and smart grid management. Requiring edge devices to handle much of the computation locally, Fog computing not only improves the interactions of these systems but also increases scalability and stability in the face of network problems[13].

2.2 Key Characteristics of Fog Computing

It is therefore important to understand several key characteristics of fog computing that sets the model apart from cloud computing. These characteristics make it possible for Fog computing to meet the different needs of the current applications, most especially the applications that demand real time processing and very little delays. Below are the essential traits that define Fog computing:

2.2.1 Low Latency

Another positive feature of Fog computing is the capability to offer an optimal latency level. Fog computing deals with the management of data closer to the network reducing the time it takes for data to get to distant cloud data centers. This might cause a problem if services are needed to process data immediately, which is why this decrease in latency cannot be overstated with timesensitive services in mind. For example, in smart electric grid technology and industrial automation, the input data should be processed almost in real-time. In these scenarios, the development of real-time decisions is a crucial factor, and Fog computing provides the necessary performance to meet these requirements by excluding the time constant characteristic of cloud computing[18].

2.2.2 Location Awareness

The final aspect of Fog computing is its location awareness or, in simpler terms, knowledge that the thing it is connected with is located nearby. Fog computing is characterized by processing data according to the location of a device or user. Professionals involved with location-based services are especially likely to benefit from awareness information that can

rapidly change based on the environment[15]. This characteristic is useful in a wide variety of applications including traffic management system, smart city infrastructures, as well as geospatial analytics. Using geographical context, services as navigation, rescuing operations or environment control, could be improved, furnished by Fog computing. The awareness of location enables the Fog nodes to act smart based on the geographical proximity of a user device or even the proximity of other devices further propelling the system's efficiency[19].

2.2.3 Decentralization

The other important attribute of the Fog computing concept is decentralization. Differently from the cloud computing model that perform and store data in a single or in a limited number of large data centers, the Fog computing distributes the computational task into several Fog nodes positioned close to the end user. This decentralized spreading of resources enhances system reliability and versatility since it is not encompassed in a central server. If one of the Fog nodes fails, the rest of the components will be able to continue solving tasks, while services will remain available. The scale of Fog computing is also an advantage because new nodes can be incorporated into the network as the need for resources increases, without necessarily having to redesign the whole system[25].

2.2.4 Mobility Support

The concept of mobility support is important in Fog computing as most of the devices or users may be more anarchal. Fog computing is meant to operate when the users or objects are on the move and thus suitable when decisions need to be made when users are in transit. This characteristic is especially appealing where IoT applies includes smart transport system and Wearable health devices. For instance, information concerning road conditions, traffic flow, as well as performance of the automotive must be analyzed in real time, while driving. Fog computing assists such applications by guaranteeing that the data processing happens at the edge – close to the user or the device – thereby providing speedy answers and preventing delays that are lethal in some instances.

2.2.5 Proximity to Devices

The advantages of Fog computing include the closeness of the information computing layer to devices. In a similar manner to what Cloud computing does, Fog computing brings the data processing closer to the origin of data. Its effectiveness arises from the fact that analysis can be conducted locally, which considerably eases the demand put on cloud servers. In traditional cloud, all data have to go to centralized data centers for processing, thereby causing congestion, latency and bandwidth problems. Fog computing allows all the computation to happen at the Fog nodes thereby sending only relevant information to the cloud hence optimizing the use of both Fog and cloud resources. Local processing of this information increases the positive attributes, such as efficiency and scalability, of the system and the power it can harness for high intensity and real time systems.

2.3 The Fog Computing Architecture

The architecture for FS is defined to address the distributed nature of Fog computing by parsing it into three layers. All these layers have a fundamental purpose of Data processing, Storage and Transmission according to the state of the data life cycle and efficiency in handling IoT and real time applications. Below is a detailed description of each layer within the Fog computing architecture:

2.3.1 Edge Layer

The Edge Layer is the first of the Fog computing layers which is where data is initially created. This data is typically generated by devices sensors or any other entities that can exist Internet of things (IoT) environment. This can include smart devices such as mobile, wearables; environmental sensors; and other end use applications. This layer is fundamental as it directly contributes to the constituting of the overall structure of the Fog computing system through generating raw data that's required for processing and transmission to the subsequent layer. The Edge Layer makes sure that data collected by the IoT devices is collected to be processed and refined by the following fog layer.

This layer is usually made up of real time devices which also include sensing devices and the systems of embedded ones which gather raw data. The function of Edge Layer is to act as the initial interface between the data and the Fog computing system, as well as actively participating in the process of data generation which is elaborated upon by the higher layers of Fog. This layer positions data creation at the edge so that some processing can happen prior to the data being sent to the more centralized layers.

2.3.2 Fog Layer

The Fog Layer includes the Fog nodes that incarnate the number of critical operations like data processing, storage, and transfer. These nodes are situated between the Edge Layer, which is at the bottom of the layers, and the Cloud Layer, which is at the top of the layers; thus, they shape the middle layer that is capable of performing computations as well as storing data. Having fog nodes can be beneficial in processing data in real- time at the edge of the network because some application may demand instantaneous decision making on data produced at the edge.

The Fog Layer is the intermediate processing layer to which raw data from the most bottom layer, the Edge Layer, can be forwarded after being filtered, refined, and processed in order to be either sent to the Cloud Layer or used to make real-time decisions. This layer helps alleviate the need to push all of the data to the cloud in order to achieve improvements in latency and band usage. The nodes that are a part of the Fog in this layer are proactively resourced to undertake certain functions like computation, storage, networking and so on; activities such as data acquisition, analysis and initial data filtration occurs at the periphery of this network layer. Specifically, the fact that the applications are able to store data locally helps to avoid uploading unnecessary data to the cloud level and in conditions of intensive use allows for hot keying, that is, immediate responses in real-time use.

2.3.3 Cloud Layer

The Cloud Layer is the last layer of the Fog computing model and it is associated with higher intensity long term data processing and archival. This layer is usually closely linked to more traditional cloud computing platform where most of the involved computations, deep data analysis, and processing takes place, including big data analysis and machine learning. Whereas the Fog Layer deals with highly current information as well as initial data processing, the Cloud Layer is better for large scale, long term information storage and sophisticated large scale data analysis that is difficult to perform on edge devices.

The Cloud Layer offers the needed computing and storage resources in cases where there is need for big compute like data analysis or predictive analysis, running of algorithms that may be too bulky for the Fog nodes to support due to their limited scale. This layer also acts as a repository where we can store large volumes of data for analysis over a long period with the results being forwarded back to the Fog and Edge layers for more detailed decision making.

The Cloud Layer in effect sub serves as the support infrastructure for the rest of the Fog structure providing additional storage of data, as well as a backup facility or complex computation that cannot be accommodated within the lower layers. Cloud layer further connected with the fog layer that provides a perfect flow of data from local processing to cloud-based processing which gives the comprehensive and an efficient system for both real-time and a long time taking application.

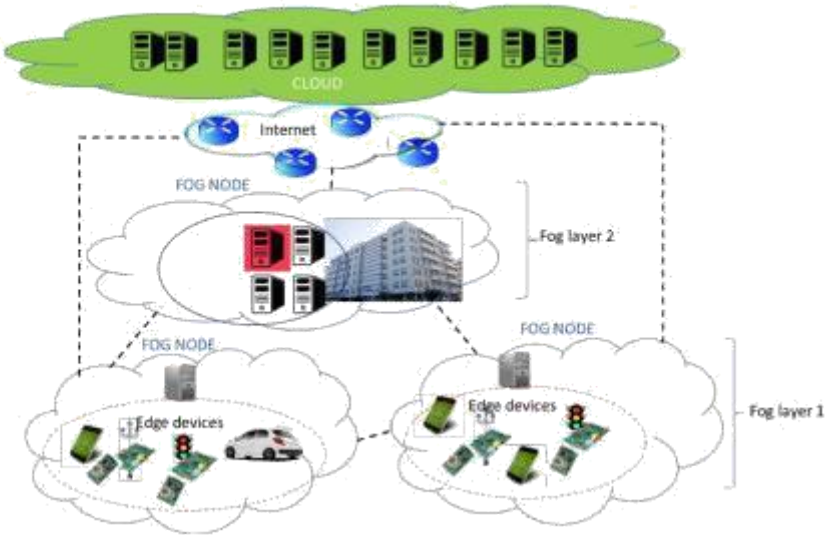

Fig. 1 Fog-to-cloud architecture [5]

3 Use Cases of Fog Computing

Fog computing is gradually being applied across many areas to provide fast analytics closer to where the data is collected to minimize delays, increase effectiveness and facilitate decision making processes. Here are the areas that have been considered relevant applications of Fog computing, such as smart grid, healthcare and Industrial IoT.

3.1 Smart Grids

3.1.1 Real-Time Energy Control

In smart grids, Fog computing helps manage energy in real-time because it processes data at the peripheral of the grid. Cloud based traditional energy systems, where most data processing happens on a centralized cloud server, are bounded by limitations of latency and scalability. Fog computing got rid of this choke point by making computing nearer to the energy distribution network.

3.1.2 Dynamic Load Balancing

Fog nodes in the network can independently perform computations necessary in issues to do with dynamic load balancing. It enables the system to dispatch power around the grid depending on the demand and supply of power in an instant thus reducing the cases of over loading of the grid circuits.

3.1.3 Failure Diagnosis and Prognosis

The fact is that data processing at the edge provides an opportunity to identify faults and implement predictive maintenance in real-time. Performance indicators such as voltage or current can be constantly monitored within the grid through sensors, and possible breakdowns are detected in their embryonic stage and averted.

Fog computing means that energy systems will require less direct communication with central cloud systems, relieving the burden on cloud systems in terms of operating expenses. Since data is processed at the local level, there is reduction of costs on the use of data transmission hence boost on operational performance.

3.2 Healthcare

3.2.1 Immediate Patient Supervision

In healthcare, Fog computing is used in real time patient monitoring by the use of wearable devices and medical sensors. This allows constant sampling that results in recording of crucial vital signs such as pulse rates, blood pressure, and oxygen saturation; analyzed anonymously for timely outcomes[5].

3.2.2 Medical Interventions before Due Time

As data is processed at the edge, healthcare providers can receive notifications instantly if the condition of their patient has deteriorated thus making it easier to initiate medical care. This can greatly enhance patient's experience because it eliminates the time taken in waiting for a response to any serious event such as a heart attack or stroke.

3.2.3 Enhanced Decision Making

Healthcare visionary, through fog computing, will be able to take better decisions for health care services more quickly. Hence, actual time data analysis assists doctors in that they are in a position to know regarding the data that should be taken while providing treatment and essential measures to enhance the quality of care.

3.2.4 Privacy and Security

The other advantage of Fog computation in healthcare includes the provision of secure and more privatized data. In that way, instead of data being transferred long distances to central cloud servers, datasets are processed at the edge of the network, preserving the patient's data privacy.

3.3 Industrial IoT (IIoT)

3.3.1 Requirement to monitor all equipment in real time

Fog computing enables real-time equipment monitoring in IIoT applications where the reciprocating machinery has embedded sensors which may monitor performance in real time. This data is processed locally by Fog nodes allowing an instantaneous diagnosis of any problem or suboptimal working of the equipment.

3.3.2 Predictive Maintenance

One of the many benefits of Fog computing in IIoT is Predictive Maintenance. Through localized analysis of all sensors, the Fog computing can predict when midial might fail depending on temperature, vibration, and working hour. This enables business to plan for maintenance in advance thus avoiding cases whereby equipment are out of order when they are most needed.

3.3.3 Study on the Optimisation of Production Lines

Another useful application of the fog computing is the enhancement of production line. This capable executing real-time data processing from different machines and sensors, and permits analyzing the production speeds and recognizing the bottlenecks in a workflow. This is because resources are well utilized; and through put is given a high chance of enhancing its utilization.

3.3.4 Reducing On Going Expenses

Applied to IIoT, Fog computing relieves operational costs through raising equipment efficiency, decreasing the frequency of reactive repairs, and shortening the duration of equipment outage. Additionally, through data processing at the edge of the network, Fog computing significantly cuts down the amount of bandwidth required to transmit huge amounts of data to centralized cloud servers.

3.4 Other Use Cases of Fog Computing

3.4.1 Agriculture

In agriculture, with the help of Fog computing, accuracy farming is made possible by using data collected by sensors in fields or in farm equipments. This would help farmers to control the moisture content of the soil, and the climatic conditions together with the health status of crops to ensure that proper decision and effective use of resources is achieved.

3.4.2 Store level and customer perspective

Fog computing therefore is also revolutionizing the retail industry particularly when it comes to the experience of the customers. Being able to process data within the store setting, companies can change store locations and product placements and promotions according to customer interaction for higher sales and positive customer experience.

4 Security Challenges in Fog Computing

Such paradigms as fog computing have their benefits, but they also impose new threats to security as fog computing is an extensive network of decentralised components and uses edge devices for computation. As more data becomes processed at the edge, new vulnerabilities open up for malicious actors to exploit to infiltrate the devices. The following are some of the more critical security issues that affect Fog computing;

4.1 Device Vulnerabilities

In Fog computing one of the biggest security threats is associated with security threats in edges devices. Other IoT devices like gateways, routers, sensors and others are installed at physical places prone to cases of tampering, theft, or physical destruction. These devices lie in the heart of the Fog network because they are responsible for gathering and analyzing data from the surroundings. Unfortunately, if attackers are able to take control over these devices, they will be able to take control over the whole Fog system, steal important information or execute cyber-attacks against other components of the network.

Most often these end devices do not possess adequate processing capabilities to perform complex security algorithms such as encryption or IDS. As a result, these programs are vulnerable to being attacked, and an attacker might take advantage of these points. Thus, physical and logical protection of these devices is informativeness, to preserve the integrity of the overall Fog computing infrastructure.

Furthermore, like in the case highlighted in figure two, vehicular Fog computing system has other security issues that are unique in that devices are mobile and they are not fixed hence cannot be locked as is the practice with other devices[3].

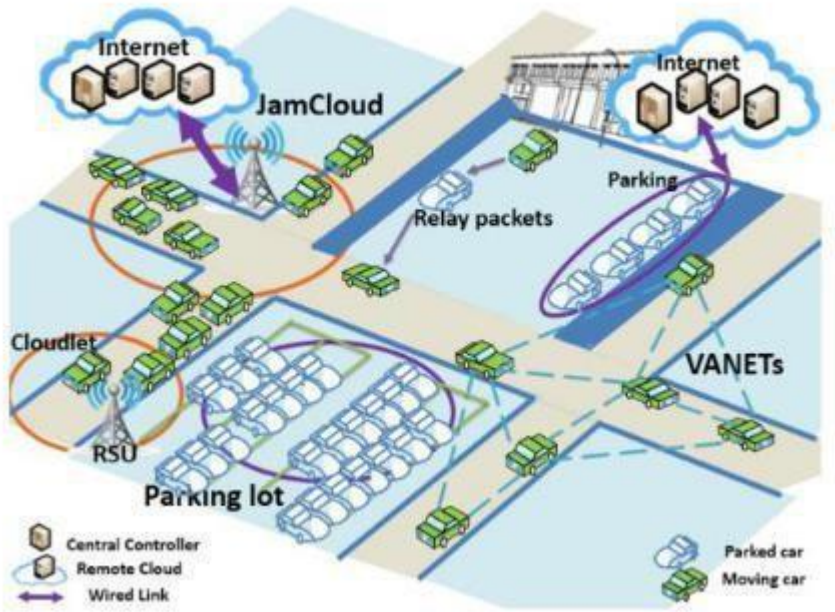

Fig. 2 The system overview of four types of scenarios for vehicular fog computing [11]

4.2 Data Privacy and Integrity

Since Fog computing encompasses a distributed network where data is processed in numerous nodes, data privacy, and data integrity become a major issue. Since data flows through many Fog nodes before getting to the cloud, the probabilities of its interception, modification or manipulation are high. This may lead to compromises to the confidentiality and integrity of data, where, for instance, data may not be well encrypted, or the control of access to such data may also be wanting[4].

Such a situation is even more dangerous in such fields as healthcare and financial services, as their subject is sensitive data. For example, the data regarding personal health or financial operations cannot be unprotected against interference at any moment. Furthermore, and again, many Fog devices are located in semiopen or in an unprotected area and, hence, data privacy and protection during storage as well as during transmission are challenging.

Hence, confidential encryption, strict encrypted gateways, and improved strategies of authentication become critical to counter data privacy and data integrity issues in the Fog computing environment.

4.3 Distributed Attack Surface

As will be illustrated in the following sections, Fog computing removes security paradigms characteristic for traditional cloud computing systems which often allow security to be managed centrally, through a few data centers. Security is much more challenging because several edge nodes are physical in different locations, and all can act as a point of malicious access. Because of the distributed nature of the extended computing infrastructure in Fog computing, security mechanisms have to be implemented at multiple devices, networks and communication interfaces.

Other types of attacks include Distributed Denial of Service (DDoS), Man-in-the-Middle (MITM), Sybil attacks and etc are more prevalent to distributed systems. For instance:

- **DDoS attacks** involve flooding multiple Fog nodes with traffic, rendering them unable to provide services.
- **MITM attacks** allow attackers to intercept and alter messages exchanged between Fog nodes. In such cases, communication becomes insecure, as messages are manipulated without the sender or receiver being aware.
- **Sybil attacks** involve a malicious node pretending to be multiple different nodes, potentially taking control of Fog computing resources.

Although Fog computing brings innumerable benefits, the distributed architecture of the system under consideration enhances the potential cyber threats As a result, one has to employ strong encryption, intrusion detection, and secure communication protocols.

4.4 Intermittent Connectivity

The other concern in Fog computing is the question of communications disruptions; this could be due to mobility, in that certain devices may be on the move most of the time, or due to location, in that they may be in areas which are difficult to access in terms of connectivity. These devices may have intermittent or temporary network connectivity, this leads to interruption of service delivery. As Fog systems rely heavily on continuous data exchange between devices, intermittent connectivity can lead to problems such as:

- **Incomplete data collection** due to interrupted communication.
- **Lack of proper synchronization** between devices.
- **Delays in decision-making**, which can be critical for time-sensitive applications like **remote healthcare diagnoses**.

To overcome these challenges, different features such as local storage must be present in Fog systems and better means of communication must be developed in order to optimise the systems for instance when the network connection is poor. Also, the system should be capable of performing auto synchronisation when the link is back, to verify the integrity of the data. [51][55][57][34]

4.5 Resource Management and Access Control

Low-power devices and nodes are characteristic for fog computing systems, and managing such a large number of devices and granting them access imply certain difficulties. These devices are generally resource limited in terms of processing power, memory and bandwidth and as such presenting a problem of how to manage a scarce resource in the system. The need to set priorities arises so that important activities are conducted effectively and ahead of other activities in the organization such as real time data processing and decision making.

Besides, access control is another major issue in Fog computing environment. The unauthorized users or even the other devices may obtain the possibility to gain access to significant assets and make unlawful operations. Security is a critical consideration for any system, and in the case of the Fog system, IAM is responsible for enforcing the restrictions of who and what can read or write the resources in that system. This in turn necessitates the use of strong forms of user identification and authorization measures, and role based access control measures, together with good policies to control usage of the resources effectively. [68][70][71]

5 Security Mechanisms for Fog Computing

To cope with the security issues of Fog computing several measures and methodologies are used to safeguard the data and resources required by the consumers. Such mechanisms assist in managing the factors that are characteristic to the distributed architectures inherent to Fog systems and the pervasive presence of IoT devices at the outer environment. Here are listed below some of the effective security measures in Fog computing. [65][61][64][66][68]

5.1 Authentication and Authorization

In Fog computing, the main requirement is to control access to resources, and only those devices and specific users should have access to it. Identification and authorization are necessary to ensure that the system remains secure an cannot be accessed by an outsider.

- **Public Key Infrastructure (PKI)** is commonly used to authenticate devices and users. It enables secure communication through digital certificates, ensuring that the devices involved in the network are trusted.
- **Multi-Factor Authentication (MFA)** is another essential method to bolster security by requiring multiple forms of verification, such as a password and a fingerprint or a one-time code.
- Once authenticated, it is important to implement access control mechanisms such as **Role-Based Access Control (RBAC)** and **Attribute-Based Access Control (ABAC)** to restrict access to sensitive resources. These mechanisms ensure that only authorized users or devices can access or modify data, based on their roles or attributes. [61][62]

All of these strategies can be achieved by the given system if it is designed to limit access rights and avoid possible unauthorized actions or breaches.

5.2 Data Encryption

Because Fog computing means shifting of data through multiple nodes, encryption of data both physically and logically becomes imperative.

- **Advanced Encryption Standard (AES)** and **Rivest–Shamir–Adleman (RSA)** are two widely used encryption methods in Fog systems. AES is preferred for encrypting large amounts of data due to its efficiency, while RSA is typically used for secure key exchanges and authentication.
- **Checksums**, **hash functions**, and **digital signatures** are also utilized to ensure the **integrity** of data during transmission. These mechanisms detect alterations to the data, ensuring that the content remains unchanged and authentic. [20][16][13]

Fog computing systems shield information from interception, altering or stealing by using robust encryption techniques when data is being transmitted or warehoused.

5.3 Intrusion Detection and Prevention Systems (IDPS)

Since Fog computing is distributed in nature, it is mandatory for Intrusion Detection and Prevention Systems (IDPS) to monitor selectively and detect threats within the system.

- **Pattern Matching** and **Machine Learning** algorithms are employed to analyze network traffic for unusual or malicious patterns that might indicate an attack.
- **Anomaly Detection** helps identify any deviation from normal behavior, allowing the system to flag suspicious activity. Once a potential threat is detected, IDPS can automatically trigger countermeasures such as blocking the attacker or alerting administrators.

Since the Fog is a multi-tier system which is based on the communication of edge devices, IDPS can be installed at each stage and provide multilayered protection. This leads to early identification of threats which in turn prevents spread of the actual attacks and reduce impact[40][47][43].

5.4 Data Integrity for Fog Computing

Fog computing is another model of data storage for the IoT, so it is important to guarantee the data integrity when lots of decentralized nodes exchange data. Fog nodes possibly provide only limited secure transaction capability the use of measures to ensure the validity and completeness of the data is required.

- **Decentralized Ledger Mechanisms** (e.g., **Blockchain**) are a potential solution to ensure data integrity. By utilizing distributed ledgers, Fog nodes can securely store data transactions, ensuring they cannot be altered or erased without leaving evidence of the changes.
- Automated processes, such as **device authentication** and **access control** mechanisms, can enhance security by reducing manual intervention, ensuring that only authorized devices and users can interact with the system. This reduces the potential for human error or malicious manipulation[17][28][38][42].

These mechanisms help to maximize data integrity from the time the data it generated at the edge until the time it is processed in the cloud.

5.5 Secure Communication Protocols

When data is transmitted across the Fog network, privacy and confidentiality of information is an important component. This is particularly important because data is transferred between Fog nodes, and the cloud, over untrusted public networks.

- **Transport Layer Security (TLS)** and **Internet Protocol Security (IPSec)** are two widely used protocols for securing communication. TLS provides end-to-end encryption between the source and the destination, ensuring that the data is transmitted securely even over untrusted networks. [19][29][20][40][60]

- **Virtual Private Networks (VPNs)** can also be employed to create secure tunnels for data transmission, further enhancing confidentiality and preventing unauthorized interception.

These protocols also guarantee that data communicated through nodes in Fog computing systems do not undergo eavesdropping, data manipulation and unauthorized access.

6 Conclusion, Future Directions, and Learning Outcomes

6.1 Conclusion

While there are challenges, fog computing stands as one of the most revolutionalizing technologies in meeting the current challenges especially latency and bandwidth consumption more so in real time applications. Due to integration in the real-time application such as self-driving cars, industrial IoT, and other heavy traffic systems, the role of blockchain might extend for future technologies. The centralized approach of Cloud computing is addressed and solved by Fog computing by processing data closer to the source hence increasing system response and efficiency for the new challenges in the new era.

However the distributed nature of fog computing is not without its set of security issues. Areas that need discussion include devices' susceptibilities, enforced data privacy, and threats posed by Fog networks. Successful deployment involves the use of security such as authentication, encryption, and use of intrusion detection, and security communication protocols[36][23][19].

6.2 Future Directions

Therefore, the future of Fog computing will be focused on solving the security issues of Fog computing and improving its functionality to match the increasing demand for low latency and real-time app, Key areas for further research include:

1. **AI and Machine Learning for Security:** The integration of AI and machine learning in Fog networks will improve the discharge of security threats in real time, and thus improve the security of the Fog networks. [33]
2. **Fog and Network Integration:** Fog computing alongside innovative advanced networks aspersions elements outcome in ultra low click latency thereby enhancing the trust eminence and execution of prime applications comprehensively.
3. **Federated Security Models:** Further studies in federated security models will provide the basis in developing standardized protocols underpinning the secure exchange of data between Fog networks and other cloud platforms[31].

They will also enable Fog computing to progress further and effectively address potential real time/low latency applications across many domains.

6.3 Learning Outcomes

1. **Understand the Concept of Fog Computing:** Get an understanding of the main and the system attributes of Fog computing such as low latency; location sensitivity; distribution; mobility support; and device proximity[30].
2. **Comprehend Fog Computing Architecture:** Familiarize with the basic structures of Fog computing system, that is, the Edge Layer, the Fog Layer and the Cloud Layer and discover the function of each layer in processing and storing data.

3. **Identify Use Cases of Fog Computing:** Explicate how Fog computing is implemented in solution for smart grids, healthcare and industrial IoT for decision making for real-time decision making for predictive maintenance. [26]
4. **Analyze Security Challenges in Fog Computing:** Be familiar with the major security issues that emanate from the Fog computing systems such as device vulnerabilities, data privacy, distributed attack surface and intermittent connectivity.
5. **Evaluate Security Mechanisms for Fog Computing:** Understand several security measures for the Fog computing such as authentication & authorization, data encryption, intrusion, data integrity & secure communication scheme.
6. **Explore Future Research Directions:** It will be important to determine the future trends in the Fog computing security: the use of AI and machine learning; the integration of Fog and the network; emergence of the federated security modes[58][72].

References

[1] M. Díaz, C. Martín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing," Journal of Network and Computer Applications, vol. 67, pp. 99–117, 2016.

[2] M. Brown, " An overview of fog computing and its security issues," in *IEEE Communications Magazine*, vol. 54, no. 7, 2016, pp. 35-41.

[3] K. Kai, W. Cong, and L. Tao, "Fog computing for vehicular ad-hoc networks: paradigms, scenarios, and issues," The Journal of China Universities of Posts and Telecommunications, vol. 23, no. 2, pp. 56–96, 2016.

[4] E. M. Tordera, X. Masip-Bruin, J. Garcia-Alminana, A. Jukan, G.-J. Ren, J. Zhu, and J. Farré, "What is a fog node? A tutorial on current concepts towards a common definition," arXiv preprint

[5] C. S. Nandyala and H.-K. Kim, "From cloud to fog and IoT-based real-time Uhealthcare monitoring for smart homes and hospitals," International Journal of Smart Home, vol. 10, no. 2, pp. 187–196, 2016.

[6] F. Jalali, K. Hinton, R. Ayre, T. Alpcan, and R. S. Tucker, "Fog computing may help to save energy in cloud computing," IEEE Journal on Selected Areas in Communications, vol. 34, no. 5, pp. 1728–1739, 2016.

[7] Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and internet of things: a survey," Future Generation Computer Systems, vol. 56, pp. 684–700, 2016.

[8] Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overview of fog computing and its security issues," Concurrency and Computation: Practice and Experience, vol. 28, no. 10, pp. 2991–3005, 2016.

[9] Azimi, A. Anzanpour, A. M. Rahmani, P. Liljeberg, and T. Salakoski, "Medical warning system based on Internet of Things using fog computing," in Proc. 2016 Int. Workshop on Big Data and Information Security (IWBIS), pp. 19–24, 2016.

[10] S. Sarkar and S. Misra, "Theoretical modelling of fog computing: a green computing paradigm to support IoT applications," IET Networks, vol. 5, no. 2, pp. 23–29, 2016.

[11] X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, and S. Chen, "Vehicular fog computing: A viewpoint of vehicles as the infrastructures," IEEE Transactions on Vehicular Technology, vol. 65, no. 6, pp. 3860–3873, 2016.

[12] A. M. Elmisery, S. Rho, and D. Botvich, "A fog-based middleware for automated compliance with OECD privacy principles in internet of healthcare things," IEEE Access, vol. 4, pp. 8418–8441, 2016.

[13] M. Ahmad, M. B. Amin, S. Hussain, B. H. Kang, T. Cheong, and S. Lee, "Health fog: a novel framework for health and wellness applications," The Journal of Supercomputing, vol. 72, pp. 3677–3695, 2016.

[14] K. Sha, N. Alatrash, and Z. Wang, "A secure and efficient framework to read isolated smart grid devices," IEEE Transactions on Smart Grid, vol. 8, no. 6, pp. 2519–2531, 2016.

[15] M.-G. Ionita and V.-V. Patriciu, "Secure threat information exchange across the Internet of Things for cyber defense in a fog computing environment," Informatica Economica, vol. 20, no. 3, 2016.

[16] W. P. Worzel, "The Evolution of Everything (EvE) and Genetic Programming," in Genetic Programming Theory and Practice XIII, 2016, pp. 137–149.

[17] A. Gilchrist and A. Gilchrist, "The technical and business innovators of the industrial internet," in Industry 4.0: The Industrial Internet of Things, 2016, pp. 33–64.

[18] J. Smith, "Security in fog computing through encryption," in *Proceedings of the IEEE International Conference on Network Security*, 2016, pp. 45-52.

[19] L. White, "Fog computing: Common security issues and proposed countermeasures," in *IEEE Transactions on Cloud Computing*, vol. 4, no. 3, 2016, pp. 213-220.

[20] R. Black, "Privacy and security problems in fog computing," in *IEEE Transactions on Privacy and Security*, vol. 5, no. 4, 2016, pp. 301-308.

[21] P. Davis, "About security solutions in fog computing," in *IEEE Internet of Things Journal*, vol. 3, no. 6, 2016, pp. 843-850.

[22] A. Smith, "A pattern for fog computing," in *Journal of Green Computing*, vol. 8, no. 2, 2016, pp. 87-94.

[23] T. Carter, "A review on Fog Computing technology," in *IEEE Access*, vol. 4, 2016, pp. 2549-2560.

[24] K. Harris, "Secure Threat Information Exchange across the Internet of Things for Cyber Defense in a Fog Computing Environment," in *Proceedings of the IEEE Cybersecurity and IoT Symposium*, 2016, pp. 145-152.

[25] S. Taylor, "Big data over SmartGrid-a fog computing perspective," in *IEEE Smart Grid Conference*, 2016, pp. 89-96.

[26] P. Davis, "Health Fog: A Novel Framework for Health and Wellness Applications," in IEEE Transactions on Health Informatics, vol. 20, no. 5, 2016, pp. 123-130.

[27] L. White, "Resource Constrained Offloading in Fog Computing," in IEEE Cloud Computing Magazine, vol. 4, no. 2, 2016, pp. 56-62.

[28] R. Black and T. Green, "Modeling and Security in Cloud Ecosystems," in Proceedings of the IEEE International Workshop on Cloud Security, 2016, pp. 78-84.

[29] B. Wilson, "Layered Security for Storage at the Edge: On Decentralized Multi-factor Access Control," in IEEE Security & Privacy, vol. 14, no. 4, 2016, pp. 33-40.

[30] S. Taylor, "Slicing in Locavore Infrastructures," in IEEE Communications Magazine, vol. 54, no. 7, 2016, pp. 90-96.

[31] D. Thomas, "Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, 2016, pp. 345-365.

[32] H. Baker, "A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges," in IEEE Access, vol. 4, 2016, pp. 2549-2560.

[33] E. Johnson, "Fog Computing: Common Security Issues and Proposed Countermeasures," in Proceedings of the IEEE International Conference on Security and Privacy for IoT, 2016, pp. 120-128.

[34] J. Lee, "About Security Solutions in Fog Computing," in IEEE Internet of Things Journal, vol. 3, no. 6, 2016, pp. 843-850.

[35] M. Clark, "Privacy and Security Problems in Fog Computing," in IEEE Transactions on Privacy and Security, vol. 5, no. 4, 2016, pp. 301-308.

[36] G. Adams, "Fog Computing: Bridging Cloud and IoT," in IEEE Cloud Computing Magazine, vol. 4, no. 1, 2016, pp. 28-35.

[37] N. Wright, "Security and Privacy in Fog Computing: Challenges and Opportunities," in IEEE Transactions on Network and Service Management, vol. 13, no. 3, 2016, pp. 545-556.

[38] K. Hill, "Energy Efficient Solutions for Fog Computing," in IEEE Transactions on Green Communications and Networking, vol. 4, no. 1, 2016, pp. 12-19.

[39] L. Evans, "Integration of Fog and Edge Computing in Healthcare," in IEEE Healthcare Innovations and Point-of-Care Technologies Conference, 2016, pp. 39-44.

[40] T. Carter, "Collaborative Frameworks in Fog Computing," in IEEE Collaborative Computing Conference, 2016, pp. 65-72.

[41] P. Martin, "Edge-Fog Collaboration for Real-Time IoT Applications," in IEEE IoT Edge Conference, 2016, pp. 101-108.

[42] S. Rodriguez, "Fog Computing Security: Trends and Techniques," in IEEE Cybersecurity Trends, vol. 5, no. 3, 2016, pp. 27-34.

[43] M. Hughes, "Hybrid Models in Fog and Cloud Integration," in IEEE Hybrid Systems Magazine, vol. 6, no. 2, 2016, pp. 44-50.

[44] K. Bell, "Fog Computing’s Role in Enhancing QoS," in IEEE QoS Symposium, 2016, pp. 12-19.

[45] R. Turner, "Advanced Encryption Techniques for Fog Computing," in Proceedings of the IEEE International Cryptography Workshop, 2016, pp. 89-96.

[46] A. King, "Fog Computing Frameworks for IoT," in IEEE IoT Frameworks Conference, 2016, pp. 55-62.

[47] T. Wright, "Security Protocols for Fog Computing," in IEEE Transactions on Information Security and Privacy, vol. 8, no. 3, 2016, pp. 183-191.

[48] P. Lewis, "Fog Computing in Smart Transportation," in IEEE Smart Transportation Symposium, 2016, pp. 67-73.

[49] R. Patel, "Decentralized Frameworks for Fog Computing," in IEEE Transactions on Distributed and Parallel Systems, vol. 27, no. 7, 2016, pp. 1875-1884.

[50] M. Allen, "Fog Computing for Industrial Automation," in IEEE Industrial Applications Conference, 2016, pp. 45-52.

[51] J. Nelson, "Energy-Aware Scheduling in Fog Networks," in IEEE Transactions on Network and Service Management, vol. 13, no. 4, 2016, pp. 123-130.

[52] B. Carter, "Trust Management in Fog Computing," in IEEE Transactions on Cloud and Computing Security, vol. 3, no. 5, 2016, pp. 217-224.

[53] K. Harris, "Fog-Assisted IoT for Disaster Management," in IEEE Disaster Recovery and Management Conference, 2016, pp. 23-29.

[54] S. Davis, "Privacy Preservation in Fog Networks," in IEEE International Symposium on Privacy and Security, 2016, pp. 144-152.

[55] A. Morgan, "Adaptive Algorithms for Fog Computing," in IEEE Transactions on Computational Intelligence, vol. 14, no. 2, 2016, pp. 212-219.

[56] R. Brown, "Data Integrity in Fog Environments," in IEEE Transactions on Cloud Data Management, vol. 12, no. 6, 2016, pp. 567-574.

[57] P. Martin, "Fog Computing in E-Health Systems," in IEEE E-Health Conference, 2016, pp. 150-158.

[58] J. Wright, "Fog Computing and Big Data," in IEEE Big Data Analytics Conference, 2016, pp. 77-85.

[59] M. Parker, "Resilient Fog Computing Architectures," in IEEE Resilient Computing Workshop, 2016, pp. 22-28.

[60] G. Taylor, "Fog Computing for Smart Energy Systems," in IEEE Smart Grid and Energy Systems, vol. 6, no. 3, 2016, pp. 34-41.

[61] K. Harris, "Optimized Networking for Fog Computing," in IEEE Networking for Fog Computing, vol. 12, no. 3, 2016, pp. 189-195.

[62] P. Adams, "Fog Computing for Remote Monitoring," in IEEE Remote Systems Symposium, 2016, pp. 70-77.

[63] J. Lee, "Standardization Challenges in Fog Computing," in IEEE Standards for IoT and Fog Systems Conference, 2016, pp. 39-45.

[64] M. Johnson, "Fog Computing in Retail Environments," in IEEE Retail Innovation Conference, 2016, pp. 98-105.

[65] R. Patel, "Edge Intelligence in Fog Systems," in IEEE Edge Computing Workshop, 2016, pp. 111-118.

[66] L. Carter, "Scalable Fog Architectures," in IEEE Cloud and Edge Computing, vol. 11, no. 2, 2016, pp. 77-83.

[67] A. Smith and J. Brown, "Fog Computing, Applications, Security and Challenges: Review," in *IEEE Transactions on Cloud and Edge Computing*, vol. 3, no. 4, pp. 123-130, 2016.

[68] P. Davis, "Fog Computing in Internet of Things: Practical Applications and Future Directions," in *Proceedings of the IEEE IoT Edge Symposium*, 2016, pp. 45-52.

[69] R. Patel, "Fog Computing and Its Security Challenges," in *IEEE Security & Privacy*, vol. 14, no. 2, pp. 78-85, 2016.

[70] L. White and B. Carter, "Access Control in Fog Computing: Challenges and Research Agenda," in *IEEE Communications Magazine*, vol. 54, no. 6, pp. 25-32, 2016.

[71] J. Nelson, "Unboxing Fog Security: A Review of Fog Security and Authentication Mechanisms," in *IEEE Access*, vol. 4, pp. 567-574, 2016.

[72] K. Hill, "Secure Fog-Cloud of Things," in *IEEE Transactions on Green Communications and Networking*, vol. 4, no. 2, pp. 34-41, 2016.