Volume: 13 Issue: 06 Pages: 5188-5196(2022) ISSN: 0975-0290

A State-of-the-Art Review on Fog Computing Architecture, Applications, and Security Issues

Bipesh Subedi
Department of Computer Science and Engineering, Kathmandu University, Dhulikhel, Kavre, Nepal
Email: bipeshrajsubedi@gmail.com
Gajendra Sharma
Department of Computer Science and Engineering, Kathmandu University, Dhulikhel, Kavre, Nepal
Email: gajendra.sharma@ku.edu.np

ABSTRACT

Advancement in IoT and cloud technology has opened room for various application services in different areas. With such popularity, the volume of data increases immensely and it is infeasible for cloud technology to provide real-time services in some cases. Fog computing is an extension of cloud technology which provides real-time and time-sensitive services. Data processing is done at fog nodes that allow seamless connectivity and application services. In this paper, various fog computing architectures, applications, and security issues are discussed. It aims to provide a comprehensive review of various aspects of fog computing.

Keywords - **Cloud Computing, Fog Computing, Security, Smart Agriculture, Smart Healthcare**

Date of Submission: Apr 17, 2022 Date of Acceptance: Jun 04, 2022

1. INTRODUCTION

Internet of Things (IoT) has gained immense popularity in recent years. Similarly, cloud computing has attracted various businesses and companies by providing on-demand computing power and storage with high scalability [1]. Cloud provides three kinds of services: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Cloud computing can be integrated with IoT devices to provide cloud as well as other services to the IoT nodes [1]. With the increasing use of smart devices, IoT technology, and near-user edge devices which requires minimal latency, high data processing and aggregation in a distributed way, the centralized cloud computing technology needs to be improvised to provide an effective solution [2]. Fog Computing can be considered as an extension of cloud computing technology and was first introduced by CISCO in 2010. Fog computing resembles the cloud computing architecture with some changes in the lower level [3]. It is a decentralized network of weak performing computing equipment to solve the problems such as high latency, overloaded network bandwidth, and overloaded centre servers [4]. Fog technology cannot exist alone as it co-exists with cloud technology and resides near the IoT or edge-user devices [3]. It only stores the recent and most used data to serve the end devices. It can be considered the future of cloud computing as the end devices sensitive to real-time transmission and delay cannot be efficiently served by cloud technology.

Furthermore, the seamless data generated from sensors, wearable devices, instant messaging systems, social networks etc. constitute to the Big data. In some cases, cloud processing technologies are not able to process the big data whereas in other cases the data collected by IoT nodes are not feasible to transfer to the cloud technology for computation [5]. Such issues are responsible for causing latency and overuse of bandwidth. The fog computing model is introduced to address those issues. It has a great future because of the excessive use and dependency on IoT devices in today's world. Different sectors including agriculture, health, industry, education and many more are using IoT devices to solve real-life problems. With the increasing need and development of network applications, fog computing can be an alternative to solve issues in processing and transmitting data in mission-critical systems.

1.1 Characteristics of Fog Computing

Fog Computing technology has various features. [2][6] have mentioned the important characteristics of this technology in their research. Some of the main characteristics are described as follows:

- Bandwidth: It saves the bandwidth as it resides towards the edge of the network to process data between cloud and end nodes which reduces redundancy, pre-processing of data, important information extraction and many more. Moreover, the local jobs are executed in fog nodes which significantly reduces the segment of transferring data.

- Geographical Distribution: The fog computing technology is widely distributed and consists of many nodes. Therefore, they are able to keep track of the end devices at different locations as well as serve these devices in real-time more efficiently.

- Heterogeneity and Interoperability: Fog computing is capable of acquiring and collecting heterogeneous data from various network applications. It also supports interoperability between various fog computing nodes using different protocols and services.

- Less Energy Consumption: The topographically distributed fog computing nodes do not require a cooling mechanism because of the minimal heat generation. Moreover, fog nodes use less power reducing energy consumption and cost. It can also be considered a platform for green computing.

- Real-Time Interactions: Real-time interactions with minimal latency are supported by fog computing instead of traditional batch processing.

- Scalability: Fog computing is scalable as it is adaptive according to the changing requirements and conditions such as variations in network conditions, changes in data-load, resource pooling and so on.

1.2. Benefits of Fog Computing

Fog computing comes with various benefits which are highlighted by [7] and described as follows:

- Latency: Fog computing resides near the user-end and deals with the local computation of data. Thus, decreasing latency in real-time applications.

- Privacy: Privacy and security of data can be maintained as confidential data can be filtered before sending it to the cloud after local tasks execution.

- Resilient to Cloud/Network Failure: Fog computing deals with cloud or network failure and provides mechanisms for safe application and data recovery.

- Inevitability: Development in ICT has increased the use of IoT devices which increases the load of the cloud as data and nodes are increasing with the application. Fog computing assists cloud technology to cope with those changes.

1.3. Fog Node

The fog node is a core component of the fog architecture which consists of physical as well as virtual components which are distributed and deployed near end devices to provide computing resources. The physical components include routers, gateways, servers etc. whereas virtual components include virtual machines, virtual switches, cloudlets etc. Fog nodes are aware of their geographical location and can be deployed in a centralized, decentralized, or stand-alone manner. The fog nodes can communicate with each other and provides data communication and management services. The fog node architecture service model provides Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) which is similar to cloud technology. Moreover, fog node deployment models include Private fog nodes, Community fog nodes, Public fog nodes, and Hybrid fog nodes [2].

The remainder of this paper is arranged in the following order: Section II discusses the various fog architectures, Section III presents its application, Section IV talks about the security issues, and Section V & VI consists of discussions and a conclusion part.

2. ARCHITECTURE

Many researchers have proposed different architectures for fog computing in recent years. In this section, five major architectures are discussed based on the systematic review of the existing related works.

2.1.3-Layer Architecture

Various works have been done on 3-layer architecture in recent years. [6][8][9] have proposed a fog system using 3-layer architecture in their research. It consists of three major layers: Cloud layer, Fog layer, and End-user/Edge/Terminal layer. The edge/terminal layer consists of the end-user or IoT devices such as cell phones, sensors etc. It senses and captures the information that is further transferred to the upper tier. The fog layer is the intermediate layer between the cloud and end-users which consists of many fog nodes

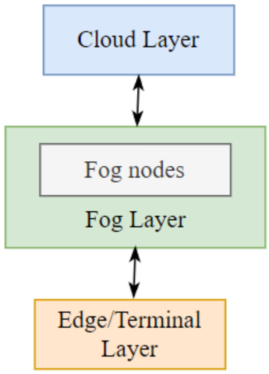

Fig. 1 3-Layer Architecture

(routers, gateways, servers, access points, base stations etc.). It provides connectivity for delivering services in stationary as well as moving states. The main function of fog nodes is to process time-sensitive data as well as transfer, quantify, and save sensed data [6]. Similarly, the cloud later provides cloud computing services for processing and storing data. Furthermore, [9] proposed a Distributed Dataflow (DDF) programming model for the IoT using fog and cloud technology. The proposed fog system is a 3-layer hierarchical architecture that includes edge nodes, compute nodes and input/output nodes. Generation of sensing data and execution of actuation messages are the basic tasks of edge nodes. Edge nodes maintain brokering interactions with Input-Output (IO) nodes, which have limited computer resources whereas computing nodes provide computational resources, and they are dynamic with programmable runtimes.

Volume: 13 Issue: 06 Pages: 5188-5196(2022) ISSN: 0975-0290

2.2. 4-Layer Architecture

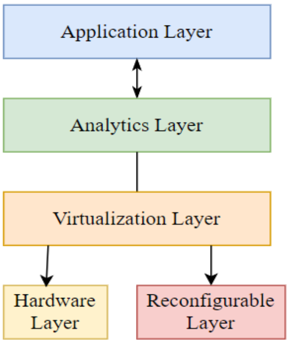

Fig. 2 4-Layer Architecture

Many works have been proposed on 4-layer architecture by [4] [10] [11] [12]. A hierarchical distributed 4-layer fog computing architecture was proposed by [10] to integrate various components for smart city applications. Layer 1 consists of data centres to provide monitoring and controlling, layer 2 consists of intermediate computing nodes, layer 3 consists of edge computing nodes, and layer 4 consists of sensing networks. The layer 2 computing nodes are connected edge devices in layer three to provide responses for hazardous events. Similarly, [4] proposed a 4-layered distributed fog computing architecture that supports multiple migration modes. The four layers consist of the Middleware layer, Registration layer, Service layer, and Management layer. A work proposed by [11] also shows a 4-layered fog node architecture consisting of a Hardware and reconfigurable layer, a Virtualization layer, an Analytics layer, and an Application layer as shown in Fig. 2. The hardware layer consists of dynamic voltage and frequency scaling for adjusting the operating voltage and frequency of the hardware devices, storage controllers for database and backup, and a network module for connectivity between fog nodes and edge devices. The virtual layer consists of a virtualization manager that abstracts the hardware resources to provide a common application services interfacing layer. The analytics layer consists of a platform services module for analyzing the usage of application services, a power management module for effective utilization of edge servers, and a machine learning module for predicting hardware resource requirements. Finally, the application layer consists of application platform services, and edge server applications. Similarly, the OpenFog architecture proposed in [12] provides a system-level architecture that supports computing, storage, and networking services at the edge level. This architecture performs computation near the end devices for minimizing latency, bandwidth costs, network costs, and migration costs [5]. Furthermore, the architecture performs the collection and processing of data at the local end and sends the results to the cloud via a secured mechanism.

2.3. 5-layer Architecture

[13] proposed a 5-layer reference architecture as shown in Fig. 3. The bottom-most layer consists of sensors, edge devices, gateways, and applications. This layer is used for sensing data. The next upper layer is the network layer which is responsible for communication between end devices and the cloud. The cloud services and resources layer is responsible for data processing and resource management. A software-defined resource management layer works on top of the cloud layer for the overall management of the infrastructure as well as enabling quality of service. It deals with flow and task placement, knowledge base, performance prediction, raw data management, monitoring, profiling, resource provisioning, and security. The final and the topmost layer contains IoT applications and solutions using fog computing to deliver services and applications to the end-users.

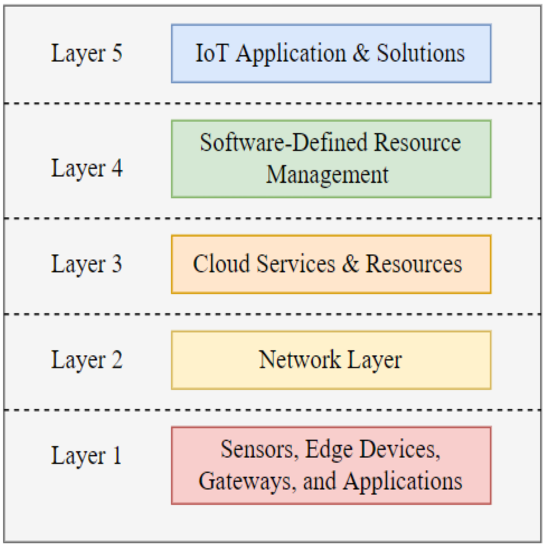

Fig. 3 5-Layer Architecture

2.4. 6-Layer Architecture

[1] proposed a 6-layer fog architecture as shown in Fig. 4. The first layer is called the physical and virtualization layer which is the bottom-most layer and deals with the generation of data using physical as well as virtual sensors. The second layer is the monitoring layer which is responsible for activity monitoring, power monitoring, resource monitoring, response monitoring, and service monitoring. The third layer is known as preprocessing layer and is responsible for data management and analysis based on which data is trimmed and filtered. The fourth layer i.e. storage layer stores data in a fog system. The data stored is mostly temporary and therefore, the cloud is preferred for permanent data storage. Moreover, the data may not reside on the fog side once it has been sent to the cloud. The security layer provides security and privacy methods to protect the data from different kinds of attacks. Applications such as smart healthcare require safe and secure communication of data as the information contains private details about the patients. Encryption/decryption mechanisms are deployed to maintain data privacy and integrity. The sixth and final layer i.e. transport layer is responsible for uploading preprocessed and secured data to the cloud.

Volume: 13 Issue: 06 Pages: 5188-5196(2022) ISSN: 0975-0290

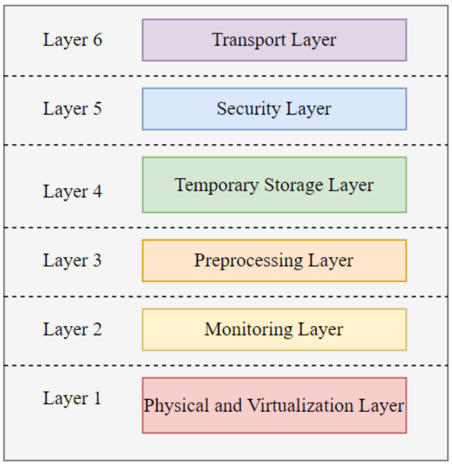

Fig. 4 6-Layer Architecture

2.5. 7-Layer Architecture

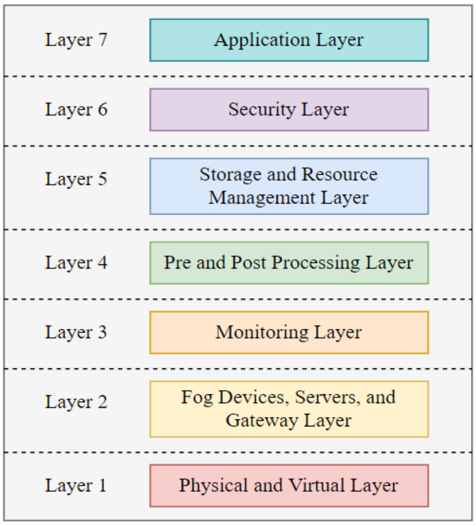

Fig. 5 7-Layer architecture

A 7-layered fog computing architecture is proposed by [14] based on the systematic literature review of the previous works as shown in Fig. 5. It consists of the Physical and Virtual layer, Fog Devices, Server and Gateway layer, Monitoring layer, Pre and Post Processing layer, Storage and Resource Management layer, Security layer, and Application layer. The first and the bottom-most layer is the physical and virtual layer which is responsible for generating information using physical and virtual sensors. The second layer manages the connectivity among devices as well as controls and maintains the fog nodes. The third layer monitors the performance of the system and provides feedback for improvements. The fourth layer is responsible for analyzing, filtering, trimming, and reconstructing data. The fifth layer performs virtualization of storage, allocation of resources, and energy management. The sixth layer is responsible for providing security measures such as authentication and encryption. Finally, the seventh layer corresponds to application services for providing cost-effective and better quality services to the users.

Table 1 provides the summary of the fog computing features supported by various architectures proposed in this section. It can be seen that architectures proposed by different research works do not support all the features and therefore, a suitable architecture should be selected which meets the requirements of the application. All the architectures mentioned in this paper support data processing near the edge devices with fog server as temporary storage and cloud as the permanent storage.

Table 1. Features Supported by various Architectures

Features	[9]	[11]	[13]	[1]	[14]
Physical devices	✓	✓	✓	✓	✓
Virtual devices	✗	✓	✗	✓	✓
Fog server	✗	✓	✗	✗	✓
Data preprocessing	✓	✓	✓	✓	✓
Scalability	✓	✓	✓	✗	✓
Reliability	✗	✗	✗	✗	✓
Monitoring	✗	✓	✓	✓	✓
Security	✗	✗	✓	✓	✓
Programmability	✓	✗	✗	✗	✗
Cloud storage	✓	✓	✓	✓	✓
Energy efficiency	✗	✓	✗	✓	✓

3. APPLICATIONS

3.1. Fog Computing in Smart Cities

The smart city concept has taken a significant focus in today's world because of its importance and effect on our daily life. With the immense development in technology and the IoT sector, the use of sensors in different sectors such as traffic management, home automation, air pollution monitoring, water management etc. has facilitated the concept of a smart city to be more realistic. All the data collected by those end devices are processed using the cloud and hence the drawbacks of the cloud are also inherited. The use of fog computing in smart cities plays a vital role because of the need for real-time and low latency applications as well as its ability to cope with the drawbacks of the cloud.

[15] has given a systematic literature review of the existing works that have been done in this field. They have compared the related works and provided some insights on the current trends and the future direction of this field. Based on their research objectives, fog computing applications are classified into three categories: Service Objective (Bandwidth Management, Latency Management, Power Management, Resource Management etc.), Application Classification (Municipal Service, Smart Citizen, Smart Education, Smart Governance etc.), and Outcome Type (Platform, Architecture, and Framework). Similarly, [10] have proposed a multi-layer fog computing architecture for big data analysis in smart cities. To check the verifiability of the proposed architecture, they have implemented a smart pipeline monitoring system using fibre optic sensors and sequential algorithms and found that the system can be implemented throughout the city on a large scale. Furthermore, a Rainbow architecture to support the smart city applications proposed by [16] suggests that applications such as noise pollution mapping, smart drainage networks, and smart streets can be evaluated using this architecture.

3.2. Fog Computing in Agriculture

Technology has penetrated almost every sector and agriculture is one of the evolving sectors among them. With the rapid development in science and information technology, many research programs are conducted to uplift traditional agricultural methods. In simple terms, Smart Agriculture is the use of modern technologies such as the Internet of Things (IoT), Wireless networks, Artificial Intelligence (AI), Location services, Robotics etc. in farming practice to increase agricultural production, sustainability, and efficiency. Smart agriculture provides various agricultural solutions such as Crop management, Livestock management, Precision farming, Smart Irrigation, Greenhouse automation, Plant and soil monitoring, and Weather monitoring [17]. A fog computing application in Agriculture and Farming called "FoAgro" is introduced in [8] for better management of the farming lands. Fig. 6 depicts the architecture of FoAgro. The fog nodes or servers are deployed along with different kinds of sensors such as moisture sensors, cameras etc. for effective farm management. The farmer can access those data with appropriate authentication and take actions based on the data shown by the devices.

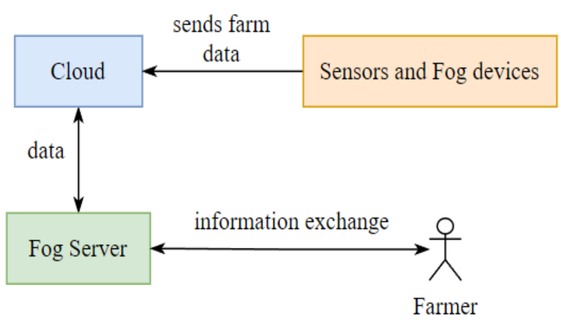

Fig. 6 FoAgro Architecture

3.3. Fog Computing in IoT

IoT devices has been used prominently in different sectors such as healthcare, transportation, agriculture, industries and many more. Such applications generate a huge amount of data which is not feasible to process using cloud technology in some cases. Fog computing acts as an intermediate between cloud and IoT devices for reliable real-time systems. [6] have mentioned the application of fog computing in IoT where fog nodes can be used to filter the data to be sent to the cloud preventing over-burdening of data transmission between the system and the cloud. Therefore, the main function of the fog nodes includes pre-processing and filtering of data, monitoring assets, and safety. Moreover, [18] have stated a distinctive use of fog computing in the Industrial Internet of Things (IIoT) where various sensors, devices, gateways etc. are used as a fog computing system to expand the productivity of a website.

3.4. Fog Computing for Smart Transportation

Smart Transportation makes the use of facilities and technology to coordinate, analyze, and control the transportation system [15]. It ensures safety, mobility, and efficiency as well as reduces fuel consumption, air pollution, and unnecessary trips. As highlighted by [15] the smart transportation system can be applied in important areas such as Traffic Management, Parking Monitoring, Public Transportation Management, Incident Detection and Monitoring, Pedestrian Management and control, Pricing, and many more. For instance, sensing the presence of pedestrians, cyclists, and the distance of the vehicles near the traffic lights can be done using fog computing [30].

Furthermore, [6] has highlighted the work of [20] where a Vehicular Ad-hoc Network (VNETs) called Fog Software Defined Network (FSDN) was proposed with features such as Programmability, Flexibility, Global Knowledge, and Scalability along with the fog capability of location awareness, and real-time interaction. Communication is augmented among vehicles, infrastructures, and base stations. This work has less consideration towards platform and application requirements and mainly focuses on infrastructure and network using fog controller as a service. Smart transportation applications (VANETs) can be used to gather transportation data for making crucial decisions on route changing, change in speed, obstacle monitoring, changing lanes and so on [21].

3.5. Fog Computing in Health Care

The concept of smart health has enabled the integration of IoT devices such as real-time sensors in the health care sector. It is a crucial field and the latency in data transmission may result in severe consequences. Therefore, the fog computing approach can be helpful in such scenarios as well as in critical systems. [8] have discussed an application called "MediFog" for detecting and predicting unusual patient situations (cardiac arrest, fall in blood pressure etc.) which uses fog computing technology. Fog servers are deployed to collect patient data which can be accessed by patients as well as hospitals. The collected data are kept private and secured for preventing any kinds of intrusion. Fig. 7 Shows the architecture of MediFog.

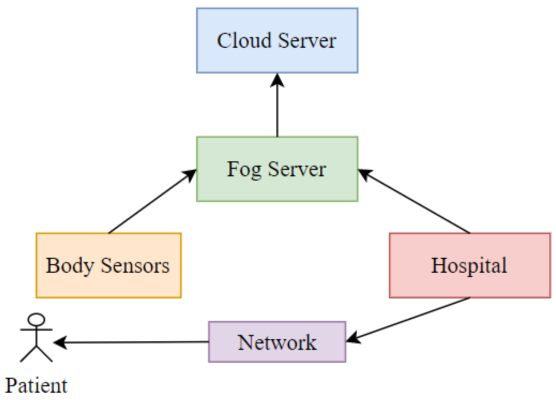

Fig. 7 MediFog Architecture

Similarly, [7] has mentioned fog computing for the Healthcare 4.0 environment using fog computing, cloud computing, and the Internet of Things to provide context-aware services to patients or users whenever required. A three-layered patient-driven architecture was proposed for real-time monitoring, processing, and transmission of data. Fog computing technology enables doctors to make smart decisions during emergencies as well as protect data without latency.

3.6. Virtual and Augmented Reality

Augmented reality blurs the line between the real and virtual worlds in the form of games and live video imagery using AR and VR devices. Different companies are adapting to this technology for the advertisement and marketing of their products [6]. It can be considered as adding virtual data to real-world platforms [19]. Augmented reality technology requires high bandwidth and high computation power in order to enhance the user experience. Fog computing is a perfect technology to incorporate those factors. It allows users to have high bandwidth data transmission and minimal latency while using their applications. Moreover, [22] proposed a game that uses augmented reality to link the brain with data using fog computing and cloud technology. The ECG headset allows reading the state of the brain which is processed using a fog system instead of sending it to the main servers which saves time.

3.7. Fog Computing as Vehicular Infrastructure

Vehicles can be used as an infrastructure for fog computing by providing computation and communication services. Smart vehicular systems rely on sophisticated networks such as Vehicular Ad-Hoc Networks (VANETs) for maintaining traffic efficiency, congestion control, safety etc. [6]. VANETs have experienced rapid growth in past years and can be used in emergency situations, content distribution for marketing and advertisements, self-driving cars, augmented reality and many more. [23] proposed a Vehicular Fog Computing (VFC) architecture where the vehicle computing power is utilized by edge or end devices near them.

4. SECURITY ISSUES

In this section, various security issues and threats to fog computing technology are discussed. As we know, fog computing inherits many features from the cloud and in that case, security issues and risks of the cloud are also inherited. Some of the major issues are discussed below.

4.1. Authentication Issues

Authentication is the process of validating a user to grant access to the service or system. It is one of the major security issues of fog computing as there needs to be secure communication among end-users, fog devices, and the cloud. The end-users or edge devices are only allowed to access the fog resources after being authenticated to the network which is very important to prevent unauthorized access [8]. The authentication process is challenging because of the power, processing, and storage constraints on network devices [24].

4.2. Trust Issues

Fog computing devices are exposed to different kinds of security threats and one of them is trust issues at the fog level. There must be some trust among all the nodes participating in the fog network. Collusion deception, trust middleware and specimen, and area-based trust are some of the trust issues highlighted by [6]. In fog computing, threats to user data, and corruption of intelligent devices in the network by malicious activities are caused due to open network environment and such procedures should be prevented to create a trusted execution environment. One of the partial solutions related to trust is the use of public key infrastructure [24].

4.3. Privacy Issues

Privacy is one of the major concerns in fog computing as sensitive data is collected, processed, and transmitted by the fog nodes which should be secured and private. The users don’t want to expose their personal data in case of any intrusion. Identity, data, usage, and location privacy are the major four aspects mentioned by [3]. The identity of the user such as name, address, phone number etc. is prone to attack for getting authentication details whereas the user data may be exposed to any untrusted party or malicious doers. Similarly, the usage details of the users can be used to identify the patterns of services used as well as the location of the user is also very sensitive data. So, all these privacy issues are related to fog computing and it is a challenging task to mitigate those issues. Moreover, controlling fog nodes via a central system is difficult due to the distributed nature of fog nodes [24].

4.4. Forgery, Tampering, and Spam

Fog systems are vulnerable to security issues such as forgery, tampering, and spam. Forgery is done by imitating the network identities to generate fake data for deception purposes which affects the network performance because of the fake data packets. Similarly, the data can tamper to degrade the network performance by delaying, modifying or dropping the transmitting data by the attacker. Spam includes fake data redundant values and data that are created and flooded by attackers to expose privacy, consume resources, and mislead users [3].

4.5. Data Integrity and Storage

Data integrity are one of the important properties in fog and cloud computing as the data sent/received by the users to/from the server should be in the exact same form. One way to achieve this is by using hashing techniques such as MD5, SHA-1, SHA-2 etc. [8]. Similarly, data stored in fog, as well as cloud databases, should be secured such that an adversary should not be able to understand the data even in case of a data leak. For this, effective encryption and decryption keys mechanism should be deployed at the fog as well as cloud ends to secure the data.

4.6. Malicious Attacks

The fog system is prone to different kinds of security breaches and malicious attacks such as Denial of Service (DoS), Man in the Middle (MITM), Sybil etc. [3]. Such attacks should be dealt with properly to ensure the safety and privacy of data. A DoS attack is a malicious attack where a huge amount of fake traffic is flooded into the fog nodes to prevent actual users from using the services. Similarly, the MITM attack works as a middle man between the fog nodes and the end-users for exchanging data without their knowledge. The attacker can spy on the users as well as change the transmitting data on behalf of the client [6]. Therefore, a fog system should be able to defend against those attacks which is a challenging task because of the size of the network as well as the open nature of the fog computing environment [24].

5. DISCUSSIONS

Different sections discussed in this study show various aspects of fog computing from its characteristics, benefits, architectures, and applications to some of its security issues. The fog computing technology indeed provides real-time transactions or interaction services with minimal latency which is crucial for critical systems. The drawback of cloud computing to serve time-sensitive applications led to the need for fog computing which works alongside cloud technology. Similarly, the architectures mentioned in this paper cover almost all the main and prevailing fog computing architectures to provide a comprehensive review of its components and functions. The most common architecture is a 3-layered fog computing architecture which is used by a majority of people. In addition to that, the popularity of 4-layered architecture is growing as it is being used for big data management as well as for smart cities application. The 5-layered, 6-layered, and 7-layered architectures are the higher layered systems that provide additional services or dedicated services for a particular module. These architectures have separate components at different layers for improving system performance, energy management, and security. Table 1 shows the features supported by various architectures. The table data shows that many architectures do not support fog servers and the majority of them are unreliable. On the other hand, data preprocessing, scalability, and cloud storage are supported by almost every architecture mentioned in section 2. All these architectures use fog computing nodes to process data near the edge level to provide seamless services and therefore, appropriate models can be chosen based on the application requirement.

From this review, it is found that 3-layer architecture is suitable if security, reliability, and energy efficiency are not an issue. 4-layer architecture is better than 3-layer architecture but has the same security and reliability issues. But it supports virtualization, energy management and fog servers unlike3-layer architecture. These two architectures are suitable for less data-sensitive tasks. Security is not an issue in 5-layer, 6-layer, and 7-layer architectures but reliability is a problem in 5-layer and 6-layer architectures. Therefore, these three architectures can be used for more data-sensitive applications. Finally, 7-layer architecture is very reliable and can be used in mission-critical system applications.

Furthermore, the recent advancements in IoT devices and cloud technology have paved a way for fog computing to be used in a variety of applications such as smart cities, smart healthcare, smart agriculture, smart transportation, vehicle computing etc. Such integration of fog nodes also poses security risks in case of authentication, data integrity, secure communication, storage etc. Some of the important risks and attacks are discussed in this paper which should be prevented for maintaining system performance, effective resource utilization, and secured transferring of data. Moreover, various challenges exist in fog computing including security, energy usage minimization, power consumption, programmability etc. Therefore, there is enough room for research in this domain and many new solutions can be devised to these problems.

6. CONCLUSION

The rise of IoT and cloud technology has raised the standards of application services. These technologies deal with an immense volume of data and therefore need the integration of a fog system. The main aim of this review is to introduce different architectures of fog computing along with its applications and security issues to provide insights on various aspects of fog computing. The paper shows the comprehensive study of fog technology which includes the proposed systems by various researchers. Fog computing is one of the important technology to manage real-time applications in this era of IoT, cloud and big data and poses immense potential as the future of cloud technology.

ACKNOWLEDGEMENTS

This paper is written for the fulfillment of the final evaluation procedure of the Distributed Operating Systems (COMP 506) course. I would like to express my gratitude to Dr. Gajendra Sharma for providing this wonderful opportunity.

REFERENCES

[1] M. Aazam, S. Zeadally, and K. A. Harras, “Fog Computing Architecture, Evaluation, and Future Research Directions,” *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 46-52, 2018. Available: 10.1109/mcom.2018.1700707.

[2] M. Iorga, L. Feldman, R. Barton, M. Martin, and N. Goren, “Fog computing conceptual model,” 2018. [Online]. Available: https://www.nist.gov/publications/fog-computing-conceptual-model

[3] A. Aljumah, T. A.-2018 7th international conference on, and undefined 2018, “Fog computing and security issues: A review,” *ieeexplore.ieee.org*.[Online].Available:https://ieeexplore.ieee.org/abstract/document/8390464/

[4] Q. Jin, R. Lin, H. Zou, F. Y.-2018 5th I. International, and undefined 2018, “A distributed fog computing architecture supporting multiple migrating mode,” *ieeexplore.ieee.org*. [Online]. Available:https://ieeexplore.ieee.org/abstract/document/8421879/

[5] R. K. Naha, S. Garg, and A. Chan, “Fog-computing architecture: Survey and challenges,” *Big Data-Enabled Internet Things*, pp. 199–224, Jan. 2020, doi: 10.1049/pbpc025e_ch10.

[6] R. Neware, U. S.-I. J. of F. Computing, and undefined 2020, “Fog computing architecture, applications and security issues,” *igi-global.com*, Accessed: Apr. 04, 2022. [Online]. Available: https://www.igi-global.com/article/fog-computing-architecture-applications-and-security-issues/245711

[7] A. Kumari, S. Tanwar, S. Tyagi, N. K.-C. & Electrical, and undefined 2018, “Fog computing for Healthcare 4.0 environment: Opportunities and challenges.[Online].Available:https://www.sciencedirect.com/science/article/pii/S0045790618303860

[8] S. Kunal, A. Saha, R. A.-S. and Privacy, and undefined 2019, “An overview of cloud-fog computing: Architectures, applications with security challenges,” *Wiley Online Libr.*, vol. 2, no. 4, Jul. 2019, doi: 10.1002/spy2.72.

[9] N. Giang, M. Blackstock, … R. L.-2015 5th I., and undefined 2015, “Developing iot applications in the fog: A distributed dataflow approach,”*ieeexplore.ieee.org*.Available:https://ieeexplore.ieee.org/abstract/document/7356560/

[10] B. Tang *et al.*, “Incorporating intelligence in fog computing for big data analysis in smart cities,” *ieeexplore.ieee.org*,2009.[Online].Available:https://ieeexplore.ieee.org/abstract/document/7874167/

[11] A. Munir, P. Kansakar, S. K.-I. C. Electronics, and undefined 2017, “IFCIoT: Integrated Fog Cloud IoT: A novel architectural paradigm for the future Internet of Things.,” *ieeexplore.ieee.org*, 2017. [Online].Available:https://ieeexplore.ieee.org/abstract/document/7948854/

[12] “OpenFog Reference Architecture for Fog Computing,” 2017. [Online]. Available: www.OpenFogConsortium.org

[13] A. Vahid Dastjerdi, H. Gupta, R. N. Calheiros, S. K. Ghosh, and R. Buyya, “Fog computing: Principles, architectures, and applications,” *Elsevier*.[Online].Available:https://www.sciencedirect.com/science/article/pii/B9780128053959000046

[14] H. Sabireen, V. N.-I. Express, and undefined 2021, “A review on fog computing: architecture, fog with IoT, algorithms and research challenges,”*Elsevier*.[Online].Available:https://www.sciencedirect.com/science/article/pii/S2405959521000606

[15] G. Javadzadeh and A. M. Rahmani, “Fog Computing Applications in Smart Cities: A Systematic Survey,” *Wirel. Networks*, vol. 26, no. 2, pp. 1433–1457, Feb. 2020, doi: 10.1007/S11276-019-02208-Y.

[16] A. Giordano, G. Spezzano, A. V.-I. C. on Smart, and undefined 2016, “Smart agents and fog computing for smart city applications,” *Springer*, vol. 9704, pp. 137–146, 2016, doi: 10.1007/978-3-319-39595-1_14.

[17] M. A. Tunc, E. Gures, and I. Shayea, “A Survey on IoT Smart Healthcare: Emerging Technologies, Applications, Challenges, and Future Trends,” Sep. 2020. [Online]. Available: http://arxiv.org/abs/2109.02042

[18] T. Zhu, S. Dhelim, Z. Zhou, S. Yang, H. N.-C. & Electrical, and undefined 2017, “An architecture for aggregating information from distributed data nodes for industrial internet of things,” *Elsevier*, 2016, doi: 10.1016/j.compeleceng.2016.08.018.

[19] A. K. Singhal and N. Singhal, “Cloud Computing vs Fog Computing: A Comparative Study,” *International Journal of Advanced Networking and Applications,* vol. 12, no. 04, pp. 4627-4632, 2021.

[20] N. B. Truong, G. M. Lee, and Y. Ghamri-Doudane, “Software defined networking-based vehicular adhoc network with fogcomputing,”*ieeexplore.ieee.org*.[Online].Available:https://ieeexplore.ieee.org/abstract/document/7140467/

[21] N. Giang, V. Leung, R. L.-P. of the 6th A. symposium, and undefined 2016, “On developing smart transportation applications in fog computing paradigm,” *dl.acm.org*, pp. 91–98, Nov. 2018, doi: 10.1145/2989275.2989286.

[22] S. José *et al.*, “Augmented brain computer interaction based on fog computing and linked data,” *ieeexplore.ieee.org*, 2014, doi: 10.1109/IE.2014.54.

[23] X. Hou *et al.*, “Vehicular fog computing: A viewpoint of vehicles as the infrastructures,” *ieeexplore.ieee.org*, vol. 65, no. 6, 2016, doi: 10.1109/TVT.2016.2532863.

[24] K. Abdulkareem, M. M.-I., and undefined 2019, “A review of fog computing and machine learning: concepts, applications, challenges, and open issues,” *ieeexplore.ieee.org*. [Online].Available:https://ieeexplore.ieee.org/abstract/document/8869895/

Biographies and Photographs

Bipesh Subedi completed his Bachelor's degree in Computer Engineering from Kathmandu University, Dhulikhel, Nepal. He is currently pursuing Masters in Computer Engineering from Kathmandu University, Dhulikhel, Nepal. His research interests are Machine Learning, Artificial Intelligence, Cloud Computing, Computer Networks, and Information Security.

Dr Gajendra Sharma completed his doctoral degree in Information Systems Engineering from Harbin Institute of Technology, China. He received a degree of Masters of Engineering in Electronics and Communication in 1997 from Moscow Technical University of Telecommunication and Informatics, Russia. He is an Associate Professor at Kathmandu University, Dhulikhel, Nepal. His research is focused on information systems, e-commerce, strategic management of information technology (IT), IT adoption, design and evaluation of IT infrastructure, strategic management of IT as well as e-governance and ethics.