Journal of Artificial Intelligence and Cyber Security (JAICS)
An International Open Access, Peer-Reviewed, Refereed Journal

Fog Computing

[1]Rakhi S. Zade, [2]Sejal N. Marke, [3]Vasudha S. Wakte, [4]Nikita F, Bankar,[5]Sanket S. Lokhande

[1] Assistant Professor Of Information Technology Engineering, Anuradha Engineering College, Chikhli

[2 3 4 5]Student, Department of Information Technology Engineering, Anuradha Engineering College, Chikhli

[1]zaderakhi2002@gmail.com, [2]Sejalmarke02@gmail.com, [3]Vasudhaswakte@gmail.com,[4]bankarnikita46@gmail.com, [5]sanketlokhande2580@gmail.com

ABSTRACT: Fog computing is a paradigm that extends cloud computing and services to the edge of the network, closer to where data is generated and consumed. This decentralized approach aims to improve efficiency, reduce latency, and address bandwidth constraints by processing data near its source rather than transmitting it to centralized cloud servers. Fog computing leverages computing resources in edge devices, routers, and base stations to perform tasks such as data storage, processing, and real time analytics. It supports a wide range of applications, including Internet of Things (IoT), smart cities, healthcare, and industrial automation, where real-time processing and low latency responses are critical. This abstract explores the key concepts, benefits, challenges, and applications of fog computing in enhancing the capabilities of distributed computing architectures. As the digital landscape evolves, fog computing continues to play a crucial role in enabling edge intelligence and improving the performance and reliability of modern networked systems.

Keywords: Security, Scalability, Open, Autonomy, RAS (Reliability, Availability, Serviceability), Agility, Hierarchy, and Programmability.

INTRODUCTION:

Fog computing or fog networking, also known as fogging, is an architecture that uses edge devices to carry out a substantial amount of computation (edge computing), storage, and communication locally and routed over the Internet backbone. Ms. Rakhi S. Zade Department of Information Technology Anuradha Engineering College Chikhli, India zaderakhi2002@gmail.com In 2011, the need to extend cloud computing with fog computing emerged, in order to cope with huge number of IoT devices and big data volumes for real time low-latency applications. Fog computing, also called edge computing, is intended for distributed computing where numerous "peripheral" devices connect to a cloud. The word "fog" refers to its cloud-like properties,

but closer to the "ground", i.e. IoT devices.Many of these devices will generate voluminous raw data (e.g., from sensors), and rather than forward all this data to cloud based servers to be processed, the idea behind fog computing is to do as much processing as possible using computing units co-located with the data-generating devices, so that processed rather than raw data is forwarded, and bandwidth requirements are reduced. An additional benefit is that the processed data is most likely to be needed by the same devices that generated the data, so that by processing locally rather than remotely, the latency between input and response is minimized. This idea is not entirely new: in non

cloud-computing scenarios, special-purpose hardware (e.g., signalprocessing chips performing fast Fourier transforms) has long been used to reduce latency and reduce the burden on a CPU. Fog networking consists of a control plane and a data plane. For example, on the data plane, fog computing enables computing services to reside at the edge of the network as opposed to servers in a data-center. Compared to cloud computing, fog computing emphasizes proximity to end-users and client objectives (e.g. operational costs, security policies, resource exploitation), dense geographical distribution and context-awareness (for what concerns computational and IoT resources), latency reduction and backbone bandwidth savings to achieve better quality of service (QoS) and edge analytics/stream mining, resulting in superior user-experience and redundancy in case of failure while it is also able to be used in Assisted Living scenarios. Fog networking supports the Internet of Things (IoT) concept, in which most of the devices used by humans on a daily basis will be connected to each other. Examples include phones, wearable health monitoring devices, connected vehicle and augmented reality using devices such as the Google Glass. IoT devices are often resource-constrained and have limited computational abilities to perform cryptography computations. A fog node can provide security for IoT devices by performing these cryptographic computations instead. SPAWAR, a division of the US Navy, is prototyping and testing a scalable, secure Disruption Tolerant Mesh Network to protect strategic military assets, both stationary and mobile. Machine-control applications, running on the mesh nodes, "take over", when Internet connectivity is lost. Use cases include Internet of Things e.g. smart drone swarms. The University of Melbourne is addressing the challenges of collecting and processing data from cameras, ECG devices, laptops, smartphones, and IoT devices with its project Fog Bus 2, which uses edge/fog and Oracle Cloud Infrastructure to process data in real-time. ISO/IEC 20248 provides a method whereby the data of objects identified by edge computing using Automated Identification Data Carriers (AIDC), a barcode and/or RFID tag, can be read, interpreted, verified and made available into the "Fog" and on the "Edge," even when the AIDC tag has moved on.[1]

2. Architecture Of Fog Computing

The Fog computing architecture consists of physical and logical elements in the form of hardware and software to implement IoT (Internet of Things) network. As shown in

figure2, it is composed of IoT devices, fog nodes, fog aggregation nodes with the help of fog data services, remote cloud storage and local data storage server/cloud. Let us understand fog computing architecture components

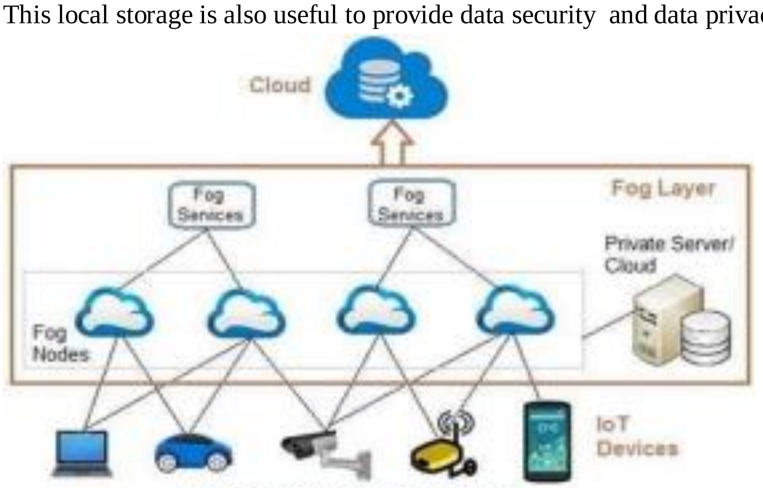
• IoT devices: These are devices connected on IoT network using various wired and wireless technologies. These devices produce data regularly in huge amount. There are numerous wireless technologies used in IoT which include Zigbee, Zwave, RFID, 6LoWPAN, HART, NFC, Bluetooth, BLE, NFC, ISA-100.11A etc. IoT protocols used include IPv4, IPv6, MQTT, CoAP, XMPP, AMQP etc.

• Fog Nodes: Any device with computing, storage and network connectivity is known as fog node. Multiple fog nodes are spread across larger region to provide support to end devices. Fog nodes are connected using different topologies. The fog nodes are installed at various locations as per different applications such as on floor of a factory, on top of power pole, alongside of railway track, in vehicles, on oil rig and so on. Examples of fog nodes are switches, embedded servers, controllers, routers, cameras etc. Highly sensitive data are processed at these fog nodes.

• Fog aggregate nodes: Each fog nodes have their aggregate fog node. It analyzes data in seconds to minutes. IoT data storage at these nodes can be of duration in hours or days. Its geographical coverage is wider. Fog data services are implemented to implement such aggregate node points. They are used to address average sensitive data.

• Remote Cloud: All the aggregate fog nodes are connected with the cloud. Time insensitive data or less sensitive data are processed, analyzed and stored at the cloud.

• Local server and cloud: Often fog computing architecture uses private server/cloud to store the confidential data of the firm. This local storage is also useful to provide data security and data privacy [2]



Fog Computing Architecture

3. Fog Computing & its Characteristics

Fog computing possess various characteristics, some of them are listed
below:

- Heterogeneity: Fog Computing is a highly virtualized platform that yields compute, storage, and networking services between end devices and traditional Cloud Computing Data Centers, typically, but not elite located at the edge of network. Compute, storage, and networking resources are the building blocks of both the Cloud and the Fog.
- Edge location: The origins of the Fog can be traced to early proposals to support endpoints with rich services at the edge of the network, including applications with low latency requirements (e.g. gaming, video streaming, augmented reality.
- Geographical distribution: In sharp contrast to the more centralized Cloud, the services and applications targeted by the Fog demand widely distributed deployments. The Fog, will play an active role in delivering high quality streaming to moving vehicles, through proxies along highways and tracks.
- Large-scale sensor networks: To monitor the environment and the Smart Grid are other examples of inherently distributed systems, requiring distributed computing and storage resources.
- Very large number of nodes, as a consequence

of the wide geo-distribution, as evidenced in sensor networks in general and the Smart Grid in particular.

Support for mobility. It is essential for many

Fog applications to communicate directly with mobile devices, and therefore support mobility techniques, such as the LISP protocol, that decouple host identity from location identity, and require a distributed directory system.

- Real-time interactions. Important Fog applications involve real-time interactions rather than batch processing.
- Interoperability and federation. Seamless support of certain services (streaming is a good example) requires the cooperation of dierent providers. Hence, Fog components must be able to interoperate, and services must be federated across domains[2]

4. CHALLENGES

There are many problems that will have to be addressed to make the fog a reality [11]First , we need to identify such problems so that researcher can concentrate on them. Some of open challenges for the fog can be listed as below:

1) Discovery/Sync: Applications running on devices may
require either some agreed, centralized point
(e.g. to establish an upstream backup if there are too few peers in our storage application;

2) Compute/Storage limitation: Current trends are improving this fact with smaller, more energyefficient and more powerful devices (e.g. one of today ‘s phones are more powerful than many high-end desktops from 15 years ago). Still new improvements are granted for nonconsumer devices;

3) Management: Having potentially billions of small devices to be configured, the fog will heavily rely on decentralized (scalable) management mechanisms that are yet to be tested at this unprecedented scale;

4) Security: The same security concerns that apply to current virtualized environments can be foreseen to affect fog devices hosting applications.

5) Standardization: Today no standardized mechanisms are available so each member of the network (terminal, edge point...) can announce its availability to host others software components, and for others to send it their software to be run;

6) Programmability: Controlling application lifecycle is already a challenge in cloud environments The presence of small functional units (droplets) in more locations (devices) calls for the right that programmers do not need to deal with these difficult[3]

4. Fog V/S Cloud

Cloud Computing: The delivery of on-demand computing services is known as cloud computing. We can use applications to storage and processing power over the internet. It is a pay as you go service. Without owning any computing infrastructure or any data centers, anyone can rent access to anything from applications to storage from a cloud service provider.

We can avoid the complexity of owning and maintaining infrastructure by using cloud computing services and pay for what we use. In turn, cloud computing services providers can benefit from significant economies of scale by delivering the same services to a wide range of customers.

Fog Computing: Fog computing is a decentralized computing infrastructure or process in which computing resources are located between the data source and the cloud or any other data center. Fog computing is a

paradigm that provides services to user requests at the edge networks. The devices at the fog layer usually perform operations related to networking such as routers, gateways, bridges, and hubs. Researchers envision these devices to be capable of performing both computational and networking operations, simultaneously. Although these devices are resourceconstrained compared to the cloud servers, the geological spread and the decentralized nature help in offering reliable services with coverage over a wide area. Fog computing is the physical location of the devices, which are much closer to the users than the cloud servers.[4]

Key Differences:

Cloud vs. fog concepts is very similar to each other. But still, there is a difference between cloud and fog computing on some parameters. Here is a point-by-point comparison of fog computing and cloud computing:

• Cloud architecture is centralized and consists of large data centers that can be located around the globe, a thousand miles away from client devices. Fog architecture is distributed and consists of millions of small nodes located as close to client devices as possible.

• In cloud computing, data processing takes place in remote data centers. Fog processing and storage are done on the edge of the network close to the source of information, which is crucial for real-time control.

• Cloud is more powerful than fog regarding computing capabilities and storage capacity. • The cloud consists of a few large server nodes. Fog includes millions of small nodes. • Fog performs short-term edge analysis due to instant responsiveness, while the cloud aims for long term deep analysis due to slower responsiveness.

• Fog provides low latency; cloud — high latency.

• A cloud system collapses without an Internet connection. Fog computing uses various protocols and standards, so the risk of failure is much lower.

• Fog is a more secure system than the cloud due to its distributed architecture.[4]

5. Security & Privacy in Fog Computing

Existing security solutions for Fog Computing: As determined in the above sections, the introduction of Fog platform functionality between end-users and the Cloud systems creates a new point for vulnerabilities, which can potentially be exploited for malicious activities. Unlike for Cloud systems, there are no standard security certifications and measures defined for the Fog computing. In addition, it could also be stated that a Fog platform:

• Has relatively smaller computing resources due to their very nature and hence it would be difficult to execute a full suite of security solutions that are able to detect and prevent sophisticated, targeted and distributed attacks;

• Is an attractive target for cyber-criminals due to high volumes of data throughput and the likelihood of being able to acquire sensitive data from both Cloud and IoT devices; and

• Is more accessible in comparison with Cloud systems, depending on the network configuration and physical location, which increases the probability of an attack occurring. The real-world applications of Fog computing and similar technologies, which are surveyed in “Related work -

current fog applications” section, are mostly motivated by functionality. However, it has also been identified that in most cases potential security measures against that can be implemented to mitigate threats are ignored.

A potential reason for this is that the security issues facing Fog systems is an infant research area, and only few of solutions are available to detect and prevent malicious attacks on a Fog platform. The below section provides an overview of such systems. Privacy preserving in Fog Computing: Research into preserving privacy in sensor-fog networks [95] consists of the following summarized steps to secure sensor data between end-user device and Fog network: • They collect sensor data and extract features;

• Fuzzing of data by inserting Gaussian noise in data at a certain level of variance to lower the chance of eavesdropping and sniffing attacks;

• Segregation by splitting data into blocks and shuffling them to avoid Man-in-the-Middle (MITM) attacks;

• Implementing Public Key Infrastructure for encrypting each data block; and • Transmit segregated data to Fog node, where data packets are decrypted and reordered. The system also includes a feature reduction ability for minimizing data communication with Fog nodes to help minimize risk. This work is of significance as it focused on preserving personal and critical data during transmission. The proposed technique can be improved by selecting an encryption and key management algorithm, focusing on those that play an important role in maintaining the privacy of data.

In addition, there is little discussion on the required computational overheads for performing extensive data manipulation (fuzzing, segregation, encryption, decryption and ordering, re ordering) before and after the communication.

This could be of significance when designing and producing a Fog system as the required computation overheads might not be available. Another important aspect to notice here is that sensors transmit data continuously, possibly over longer periods of time, and the proposed privacy framework might overload or even crash the underlying Fog system.[2]

6. Types Of Fog Computing

• Device-level Fog Computing: Devicelevel fog computing utilizes low-power technology, including sensors, switches, and routers. It can be used to collect data from these devices and upload it to the cloud for analysis

. • Edge-level Fog Computing: Edge-level fog computing utilizes network-connected servers or appliances. These devices can be used to process data before it is uploaded to the cloud.

• Gateway-level Fog Computing: Fog computing at the gateway level uses devices to connect the edge to the cloud. These devices can be used to control traffic and send only relevant data to the cloud.

• Cloud-level Fog Computing: Cloud-level fog computing uses cloud-based servers or appliances. These devices can be used to process data before it is sent to end users [3]

7. Advantages Of Fog Computing

There are several advantages to using a fog computing:

• Reduced latency: By processing data at or near the edge of the network, fog computing can help reduce latency. Fog computing works with the aim to enhance the processing, intelligence, and accumulation of data closer to the Edge devices. The proposed framework helps in reduce latency as we place a Fog node device between the cloud and the edge device where data is generated and sent to the cloud and retrieved from the cloud.

• Improved security and privacy: By keeping data and applications closer to the user, fog computing can help improve security and privacy. By keeping data and applications closer to the user, fog computing can help improve security and privacy Some countermeasures for security and privacy concerns include: Efficient encryption techniques, Intrusion detection systems, User behavior profiling, and Cryptographic techniques.

• Increased scalability: Fog computing can help increase scalability as more resources may be added at the edge of the network Fog computing is a distributed architecture that can scale to meet the needs of large and complex systems. This is because it allows for the addition of more resources at the edge of the network.[2]

8. Disadvantages OF Fog Computing

There are also several disadvantages to using a fog computing:

• Limited resources: Because fog

computing relies on devices at the edge of the network, there may be limited resources available. This can impact performance. Complex architecture: Fog computing can be complex to implement and manage because of the distributed nature of the architecture.

• Complex architecture: Fog computing can be complex to implement and manage because of the distributed nature of the architecture. Fog computing is a distributed computing architecture, as opposed to depending entirely on centralized cloud servers, which brings the processing of data, functionality of an application, and its storage closer to the network's edge, where it can be closer to the data source or an end-user device.

• Limited coverage: Fog computing can be complex to implement and manage because of the distributed nature of the architecture. Limited coverage: Because fog computing is still a relatively new technology, there may be limited coverage in terms of devices and locations that support it.[1]

9. Applications & its Benefits

og computing is an extension of cloud computing that addresses the non-viable part of cloud that leads to the incapability in meeting users demand – to process data in a matter of milliseconds thus provide actionable insight in real-time. Internet of everything (IoE), Industrial Internet of Things (IIoT), IoT applications are all the reasons for the rise of the application of fog computing. With data being the important essence in establishing sustainability in the world today, the application of fog computing had gradually become prevalent in organization.

The examples of application of fog computing

1. Smart Utility Service

The main objective smart utility service is to save cost and time through conservation of energy. Fog computing is beneficial in enabling analysis of data from the application at every minute for continuous update and addressing complication in transmission of other data heavy traffic created by IoT applications.

2. Smart Cities

The most significant examples of the application of fog computing for smart cities is traffic regulation. The traffic signals and road barriers are installed with sensors to collect data on the movement of vehicles on the road. Fog computing allows real-time data analysis that enable the traffic signal to rapidly change according to the traffic situation.

3. Healthcare

The innovation of technologies and IoT introduces the evolution of wearables. From a watch that tell time and date to a smartwatch that delivers more than just telling time and date but as well provides various users data including health condition. The wearables are also applied to the patients in hospital to give continuous information about their vitals, blood glucose levels and many more. Fog computing is useful to these wearables as it ensures data to be delivered without delay during emergency cases. 4. Video Surveillance [2]

Shopping mall and public places usually are installed with surveillance camera to provide video images on public behaviors. Surveillance camera collects big volume of data in form of video. In order to prevent latency, fog computing is essential in helping identifies abnormalities in crowd patterns and immediately alert authorities on the situation.

E-SPIN Group in the enterprise ICT solution supply, consultancy, project management, training and maintenance for corporation and government agencies did business across the region and via the channel. Feel free to contact E-SPIN for your project requirement and inquiry. Related posts that may interest you:

1. Fog computing architecture as the extension of cloud computing
2. Challenges in Implementing Fog Computing
3. The rise of Fog Computing: What is Fog Computing?
4. From edge computing to hyperscale edge computing

10. Benefits of Fog Computing:

Now that we've explained how fog computing deals with the tremendous volume of data that is generated from IoT devices and big data analytics let's look at the benefits that businesses can reap from it.

1. Reduced Latency

One main issue that businesses had to deal with while using cloud computing was latency. If the time required for the data to reach the receiver's end is great, then it can not only reduce customer satisfaction levels but also can lead to potentially life-threatening situations. Take, for instance, self-driving cars. Various sensors implanted on a driverless vehicle generate massive amounts of data in real-time. This data has to be analyzed and processed almost instantaneously after being sent to the cloud. Delayed data transmission can pose serious risks to people traveling in the vehicle. Fog computing can be useful at dealing with slow oncloud computational process. As fog computes the data on a server that is closer than the centralized data center, data transmission will become quicker, thereby eliminating the latency issue.

2. Enhanced Security

Fog computing is a decentralized computing infrastructure, which means that the servers are placed at various strategically determined locations. Such complex systems can be challenging to hack and disrupt. Hence, introducing fog computing can help organizations to bolster their cybersecurity mechanisms, thereby enhancing security for their IT environment.

3. Improved Customer Experience The ultimate goal of every business is to provide unparalleled services to customers. As, due to fog computing, the 'lag' in data transmissions is minimal, customers can enjoy prompt response and assistance for all their requests. Such support will improve customer satisfaction and enhance their overall experience.[2]

4. Use Cases of Fog Computing So far, we have explained the concepts of fog computing, what it means, and how businesses can benefit from it. Now, let's run you through some specific examples of where and how fog computing can be applied in practical use cases: 5. Smart Cities

One main challenge for smart cities is to analyze and compute the amount of data that is generated every second from millions and millions of sensors embedded throughout the city. Hence, smart cities can offer the right environment for implementing fog computing. Fog nodes are meant to process the data that is immediately required without sending everything back to the cloud servers. This being the case, the time taken for data to travel will be negligible. This means that the necessary actions will be taken in real-time, thereby helping the government and city developers to make the concept of smart cities a success in reality. For example, sensing the arrival of ambulances and changing the traffic lights to green automatically can save numerous lives.

6. Drones

There has been a tremendous buzz around drones for quite a while now. However, the concept of drones is still more theoretical than practical. The reasons for why drones haven't reached mass adoption range from inadequate safety to bandwidth and latency issues. All of these issues can be fixed easily with the help of fog computing. With fog computing, drones can be monitored and handled by users. When a drone is in transit, constant monitoring is necessary to ensure that collisions don't occur. Tracking the location and condition of drones in real time requires satellite links, which can be expensive for companies. With fog computing, the data that is generated will be processed in real-time, thereby eliminating the bandwidth .

11. Conclusion :

Fog computing, a cornerstone of decentralized computing is poised to reshape our digital landscape. By bringing computation and storage closer to data sources, it transforms how handle IoT-generated data. Exploring the future through fog computing reveals benefits like reduced latency, enhanced privacy, and efficient network utilization. Yet, challenges abound. Resource management, security, standardization, quality

of service, scalability, and energy efficiency pose hurdles. Addressing these challenges demands ongoing research and innovation. As we delve deeper into decentralized computing, fog computing's role grows pivotal. It's a journey of discovery, innovation, and problem-solving. Successfully navigating challenges is key to unlocking fog computing's potential. This journey promises a more efficient, responsive, and decentralized digital world.[4]

12. Reference:

1. https://www.wikipedia.org/
2.https://www.eccouncil.org/cybersecurityexchange/ethical-hacking/fog-computing everythingto-know/
3. https://www.sciencedirect.com/topics/computerscience/fog-computing 4. http://www.google.com/