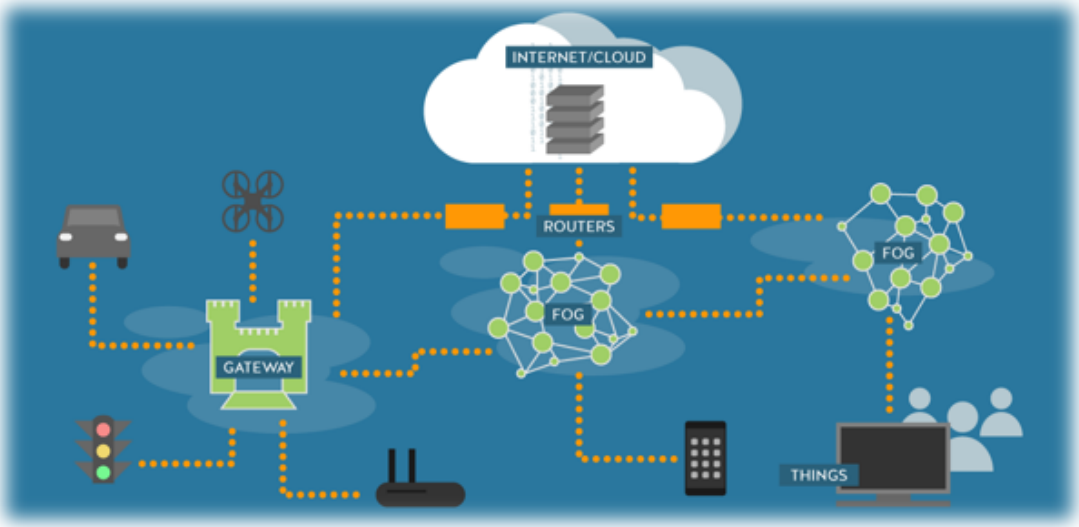

Chapter (6) Summary:

Fog Computing

Prepared by: Wasim Alfarram

University ID: 210401063

Supervised by:

Dr. Öğr. Üyesi Mehmet Erdal Özbek

(6.1) Defining Fog Computing [1]:

- What is Fog Computing?

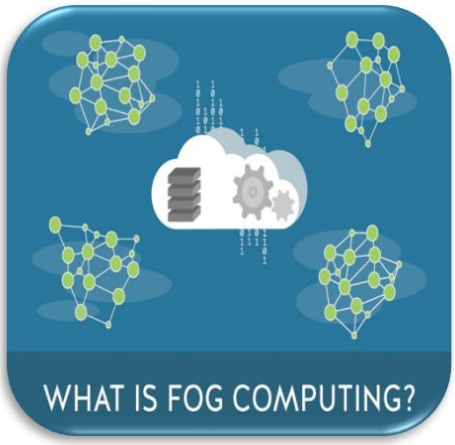

Figure (1)

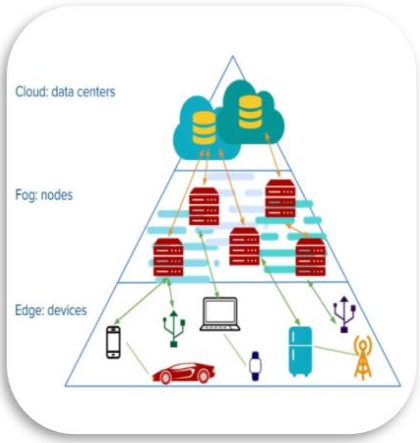

Figure (2)

Fog Computing is a decentralized computing infrastructure in which data, compute, storage and applications are located somewhere between the data source and the cloud. Like edge computing, fog computing brings the advantages and power of the cloud closer to where data is created and acted upon. Many people use the terms fog computing and edge computing interchangeably because both involve bringing intelligence and processing closer to where the data is created. This is often done to improve efficiency, though it might also be done for security and compliance reasons.
The fog metaphor comes from the meteorological term for a cloud close to the ground, just as fog concentrates on the edge of the network. The term is often associated with Cisco; the company's product line manager, Ginny Nichols, is believed to have coined the term. Cisco Fog Computing is a registered name; fog computing is open to the community at large.

• How does Fog Computing work?

Fog Networking complements – does not replace - **Cloud Computing**; fogging enables short-term analytics at the edge, while the cloud performs resource-intensive, longer-term analytics. Although edge devices and sensors are where data is generated and collected, they sometimes do not have the compute and storage resources to perform advanced analytics and machine learning tasks. Though cloud servers have the power to do this, they are often too far away to process the data and respond in a timely manner.
In addition, having all endpoints connecting to and sending raw data to the cloud over the internet can have privacy, security and legal implications, especially when dealing with sensitive data subject to regulations in different countries. Popular fog computing applications include smart grids, smart cities, smart buildings, vehicle networks and software-defined networks.
What is edge computing? Everything you need to know

• Fog Computing vs Edge Computing:

According to the OpenFog Consortium started by Cisco, the key difference between edge and fog computing is where the intelligence and compute power are placed. In a strictly foggy environment, intelligence is at the local area network (LAN), and data is transmitted from endpoints to a fog gateway, where it's then transmitted to sources for processing and return transmission.
In edge computing, intelligence and power can be in either the endpoint or a gateway. Proponents of edge computing praise its reduction of points of failure because each device independently operates and determines which data to store locally and which data to send to a gateway or the cloud for further analysis. Proponents of fog computing over edge computing say it's more scalable and gives a better big-picture view of the network as multiple data points feed data into it.
It should be noted, however, that some network engineers consider fog computing to be simply a Cisco brand for one approach to edge computing.

- ## How and Why is Fog Computing used?

There are many numbers of potential use cases for fog computing. One increasingly common use case for fog computing is traffic control. Because sensors - such as those used to detect traffic - are often connected to cellular networks, cities sometimes deploy computing resources near the cell tower. These computing capabilities enable real-time analytics of traffic data, thereby enabling traffic signals to respond in real time to changing conditions.

This basic concept is also being extended to autonomous vehicles. Autonomous vehicles essentially function as edge devices because of their vast onboard computing power. These vehicles must be able to ingest data from a huge number of sensors, perform real-time data analytics and then respond accordingly.

Because an autonomous vehicle is designed to function without the need for cloud connectivity, it is tempting to think of autonomous vehicles as not being connected devices. Even though an autonomous vehicle must be able to drive safely in the total absence of cloud connectivity, it is still possible to use connectivity when available. Some cities are considering how an autonomous vehicle might operate with the same computing resources used to control traffic lights. Such a vehicle might, for example, function as an edge device and use its own computing capabilities to relay real-time data to the system that ingests traffic data from other sources. The underlying computing platform can then use this data to operate traffic signals more effectively.

• What are the benefits of Fog Computing?

Like any other technology, fog computing has its pros and cons. Some of the advantages to fog computing include the following:

- **Bandwidth Conservation:** Fog computing reduces the volume of data that is sent to the cloud, thereby reducing bandwidth consumption and related costs.
- **Improved Response Time:** Because the initial data processing occurs near the data, latency is reduced, and overall responsiveness is improved. The goal is to provide millisecond-level responsiveness, enabling data to be processed in near-real time.
- **Network-Agnostic:** Although fog computing generally places compute resources at the LAN level - as opposed to the device level, which is the case with edge computing - the network could be considered part of the fog computing architecture. At the same time, though, fog computing is network-agnostic in the sense that the network can be wired, Wi-Fi or even 5G.

• What are the disadvantages of Fog Computing?

Of course, fog computing also has its disadvantages, some of which include the following:

- **Physical location:** Because fog computing is tied to a physical location, it undermines some of the "anytime/anywhere" benefits associated with cloud computing.
- **Potential security issues:** Under the right circumstances, fog computing can be subject to security issues, such as Internet Protocol (IP) address spoofing or man in the middle (MitM) attacks.
- **Startup costs:** Fog computing is a solution that utilizes both edge and cloud resources, which means that there are associated hardware costs.
- **Ambiguous concept:** Even though fog computing has been around for several years, there is still some ambiguity around the definition of fog computing with various vendors defining fog computing differently.

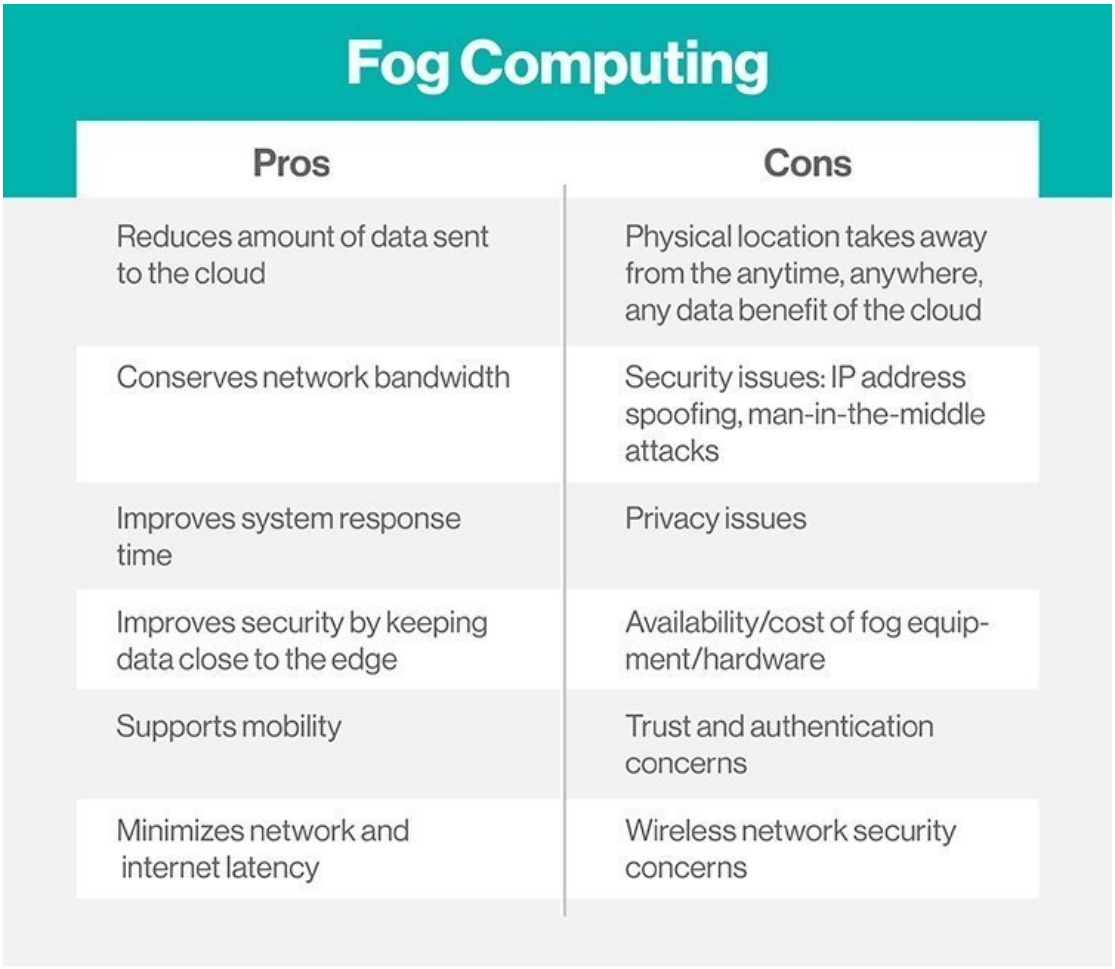

Figure (3): Fog computing conserves network bandwidth and improves system response time, but it can introduce privacy and security problems.

- Fog Computing and the Internet of Things:

Because cloud computing is not viable for many internet of things (IoT) applications, fog computing is often used. Its distributed approach addresses the needs of IoT and industrial IoT (IIoT), as well as the immense amount of data smart sensors and IoT devices generate, which would be costly and time-consuming to send to the cloud for processing and analysis. Fog computing reduces the bandwidth needed and reduces the back-and-forth communication between sensors and the cloud, which can negatively affect IoT performance.

- ## Fog Computing and the 5G:

Fog computing is a computing architecture in which a series of nodes receives data from IoT devices in real time. These nodes perform real-time processing of the data that they receive, with millisecond response time. The nodes periodically send analytical summary information to the cloud. A cloud-based application then analyzes the data that has been received from the various nodes with the goal of providing actionable insight.
This architecture requires more than just computing capabilities. It requires high-speed connectivity between IoT devices and nodes. Remember, the goal is to be able to process data in a matter of milliseconds. Of course, the connectivity options vary by use case. An IoT sensor on a factory floor, for example, can likely use a wired connection. However, a mobile resource, such as an autonomous vehicle, or an isolated resource, such as a wind turbine in the middle of a field, will require an alternate form of connectivity. 5G is an especially compelling option because it provides the high-speed connectivity that is required for data to be analyzed in near-real time.

- ## What is the history of Fog Computing?

In 2015, Cisco partnered with Microsoft, Dell, Intel, Arm and Princeton University to form the OpenFog Consortium. Other organizations, including General Electric (GE), Foxconn and Hitachi, also contributed to this consortium. The consortium's primary goals were to both promote and standardize fog computing. The consortium merged with the Industrial Internet Consortium (IIC) in 2019.

(6.2) Drivers for Fog [2]:

In particular, we see four structural patterns of applied fog computing that provide significant benefits in matters of data privacy but also for the handling of business secrets. These patterns are not necessarily new and may already be known from, e.g., hybrid clouds. In fog computing, however, they become inherent and fundamental principles of application architectures.

- Service Execution On-Premises:

A core functionality of fog computing is the movement (or: relocation) of data storage and processing away from centralized entities like cloud datacenters to on-premises edge servers. Basically, fog computing allows to decouple the software part of a SaaS business from the execution environment this software runs on. While a software executable is still provided as a service, it is executed in an environment (including hardware as well as the underlying software stack) which remains under the control of the service customer. In contrast to cloud-based models, customers therefore no longer need to completely hand-over control over their data to the service provider for being able to use said service. This, in turn, provides significant benefits for privacy as well as for the protection of business secrets. This pattern can already be found in practice. Amazon, for instance, offers ready-to-use server racks which are installed as on-premises edge servers under the physical control of the customer. These “Outpost" installations, however, run standard Amazon cloud services managed by the provider.

- Multi-Staged Filtering:

Data minimization is one of the core principles of privacy. This corresponds nicely to fog scenarios where data created near the edge is no longer streamed to the cloud for, e.g., bandwidth reasons. Instead, it is processed across multiple stages, starting at the edge, with only aggregated values arriving in the cloud. In a typical IoT scenario, for instance, sensor data is processed at the edge to either aggregate data or to filter out and discard irrelevant data items. Depending on the use-case, its data requirements, and the computational constraints it raises, this filtering might also comprise mechanisms providing local differential privacy [5, 6]. The same happens at later filtering stages within the fog before eventually arriving in the cloud for final processing. Every stage reduces the amount of data permanently stored in the cloud which will be accessible for the respective cloud providers. The pattern therefore allows to minimize the amount of data accessible for the different parties involved to the necessary minimum. In the context of business secrets, this reduces the risk of disclosure while in the context of privacy, it allows for compliance with the principle of data minimization, which is mandatory in most respective regulations such as the GDPR.

- Decoupled Data Hubs:

One of the main privacy risks in cloud computing is the correlation of data which was collected for independent purposes. Nowadays, such correlation of data – whether accidental or malicious – has become simple due to the wide availability of big data technology and the increasing accumulation of data in consolidated cloud data stores. Even though these cloud data stores typically employ sophisticated access management systems, these do not solve the underlying structural risk emanating from large centralized data lakes. When data, however, is not stored in a centralized cloud but rather distributed geographically across a multitude of fog nodes operated by different providers, joins of data sets (even accidental) become incredibly expensive. Fog-based decoupled data hubs cannot avert data correlation and inference completely (data correlation for single entities may still be possible), but it is no longer feasible to do that on a large scale. Using federated learning approaches [11], decoupled data hubs, however, still support advanced machine learning use cases such as predictive maintenance across multiple machine users. Overall, decoupled data hubs clearly counteract privacy intrusion as well as provider-side fiddling with internal business secrets.

- Fine-Granular Control of Data Placement:

Privacy legislation mandates that data may not move to certain countries. Business secrets, in turn, shall not leave company premises, and users may feel more comfortable when they can actually know and control the place where their data is stored. This is in stark contrast to the cloud which through its virtualized nature here provides only limited transparency and control. In fog computing, in contrast, the latency and bandwidth implications of geo-distribution call for explicitly exposing data placement to applications. Furthermore, the sheer number of edge locations is an enabler for really fine-grained geo-placement [12]. Respective strategies (see, e.g., [8]) can also be used to satisfy - going beyond performance- and QoS-related requirements - privacy-and security- related obligations and constraints. Furthermore, users may also welcome the option to place their data with only a subset of fog providers. All these aspects together provide the means to let application developers better meet regulatory demands and to allow users to manage the physical location of their data.

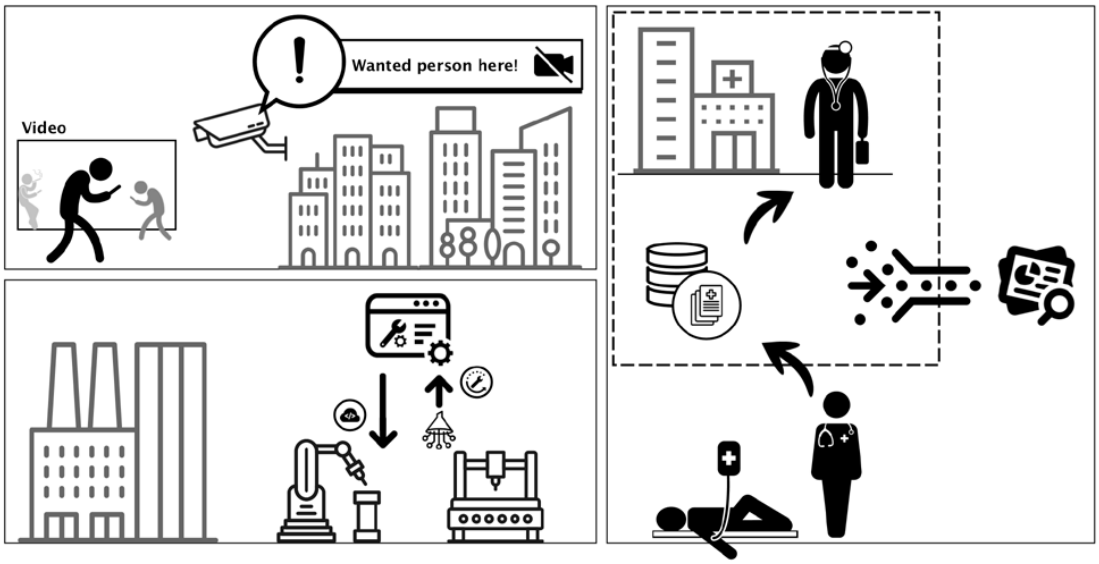

Figure (4): Fog Computing may provide data privacy and security benefits in such diverse scenarios as video-surveillance, predictive maintenance, or eHealth.

(6.3) Characteristics of Fog [3]:

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 different providers. Hence, Fog components must be able to interoperate, and services must be federated across domains.

(6.4) Enabling Technologies and Prerequisites [4]:

❖ Challenges in Computation for Dense Fog:

- Real-Time Task Decomposition and Load Balancing:

Owing to unconstrained mobility and extreme heterogeneity of the underlying computation substrate - a unique feature of the dense moving fog - efficient means are needed for on-the-fly processing, load balancing, and decomposition of computational tasks. Here, one may consider applying AI mechanisms, which are trained on the previous history of dense moving fog operations and thus able to promptly deliver a sufficiently appropriate task decomposition for the current system state.

- Distributed Computing over Unreliable Connectivity:

Despite the very dense geographical distribution, catering for proximity to end devices in fog operation may not always be feasible due to possible lack of powerful computing modules, but also because of limited connectivity in critical conditions (e.g., intermittent and prone to failure wireless links). One of the possible approaches here is to determine the minimal sufficient levels of redundancy in task decomposition, so that the final outcome can be reconstructed even in cases where a part of the intermediate computation results is not available on time.

- Communication:

It is important to continuously provide adequate rates for data exchange in the considered scenarios, given that a connected car produces tens of megabytes of data per second, while an autonomous vehicle may generate up to a gigabyte per second. Here, the dense moving fog can support the accelerated data traffic by heavily exploiting the directional high-rate communications over the mmWave bands. Dense moving fog can also provide novel ways for intelligent IoT devices to communicate with each other as well as with their proximate network infrastructure in the face of intermittent connectivity by utilizing multi-hop multi-connectivity mechanisms, thus combining the advantages of centralized and ad-hoc network topologies into a unified solution.

❖ Challenges in Communication for Dense Fog:

- (Ultra-)Low-Latency Communication:

Not limited to capacity demands, the emerging widely-deployed IoT applications may also require (ultra-) low latencies below a few tens of milliseconds: vehicle-to-everything communication, industrial and drone flight control, virtual reality and gaming services, and so on. These latency-sensitive use cases may challenge the radio communication in dense moving fog. Fortunately, recent advances in embedded AI promise to 'teach' the fog which job needs to be allocated to which resource to decrease the end-to-end delay and reduce the network loading. Here, delay-tolerant tasks may be pushed into the cloud, while time-sensitive operation can employ nearby fog devices, thus allowing the data to reside close to where it is being generated.

- Reliable Data Exchange Over Opportunistic Connectivity:

To facilitate dynamic management of computing, networking, and storage functionalities, dense moving fog architecture needs to exercise real-time control along the continuum between the data centers and the end devices. More flexible multi-hop and multi-connectivity solutions enabled over softwarized 5G radio networks are thus envisioned to address this challenge. However, these mechanisms are currently at the early stages of their development and hence call for further research. This includes determining the optimal degree of multi-connectivity (the number of simultaneous links) in particular operating conditions of the dense moving fog.

- Storage:

As fog infrastructures bring a plethora of cloudlike services closer to the end devices, efficient storage is crucial. Correspondingly, elastic memory capacity can be made available to various applications running on top of constrained IoT devices. Given that dimensioning of fog-aided operation is inherently flexible, the very large numbers of densely distributed and potentially mobile intelligent IoT entities may be integrated therein. Abundant storage space becomes accessible by the fog devices collectively with, for example, end nodes coalescing into ad-hoc capacity enclaves. As a result, multiple interconnected fog infrastructures that co-exist in space and time may serve as storage backup for each other by pooling various resources of the network edge, access, and end devices in proximity.

❖ Challenges in Storage for Dense Fog:

- Proactive Storage Selection Procedures:

To provide with flexible storage capabilities, dense moving fog has to enable informed and timely decisions on how to dynamically (re-)distribute the data among heterogeneous fog nodes. Here, proactive cell selection procedures, cooperative caching policies, and radio resource management strategies will be instrumental to address this challenge, achieve improved hit ratios at the edge, and thus avoid transferring massive data by reducing bandwidth consumption.

- Mobile Big Data Analytics:

Fog-enabled storage may benefit from mobile big data analysis, especially over densely distributed and increasingly heterogeneous data collection points. However, signaling overheads should be carefully controlled in this context, since the relatively frequent exchange of small-data packets (e.g., for traffic monitoring and logging purposes) may quickly deteriorate the available link budget. Hence, data collection and analysis have to be offered locally, by utilizing end devices and/ or edge-network infrastructure for more efficient micro-management. Augmenting data analytics with device-aided content sharing can further boost responsiveness and location awareness.

- Security:

Not limited to the above angles, fog infrastructures promise unique security-related opportunities. Massive and dense moving fog with already established dynamic chains of trust can act as a trusted authority for external devices and systems. In particular, the moving fog may handle the responsibilities of a trusted computation platform, a certification authority, and a secure storage for short-lived sensitive information, among many others. Fog can also facilitate localized threat monitoring, detection, and protection for its nodes as well as off er powerful proximity-based authentication mechanisms by proxying the end devices for better identity verification.

❖ Challenges in Security for Dense Fog:

- Secure Operations in a Heterogeneous Environment:

The central concern here is that of heterogeneity: multiple potentially competing service providers and consumers are utilizing distributed and dissimilar resources across a diverse collection of hardware platforms in multi-tenant environments. Therefore, advanced authorization and authentication mechanisms need to be coined, which will effectively leverage this heterogeneous medium and mediate between the fog entities. Fortunately, trusted execution environments supported by public-key infrastructures may become a suitable remedy for the above issues. Still, intelligent integration of hardware-assisted and software-centric security mechanisms remains an open research challenge for the envisioned dense moving fog.

- Dynamic Adaptation of Security Measures:

In contrast to the state-of-the-art systems primarily operating in known conditions, the prospective dense moving fog will have to handle volatile environments. Therefore, the employed security mechanisms have to continuously adapt to the current operating conditions. Facing this challenge, dense fog has to dynamically adjust its overall security level, which calls for designing new security protocols that will be ready to respond adequately to any security compromises without creating disruptions hampering safe and uninterrupted system operation.

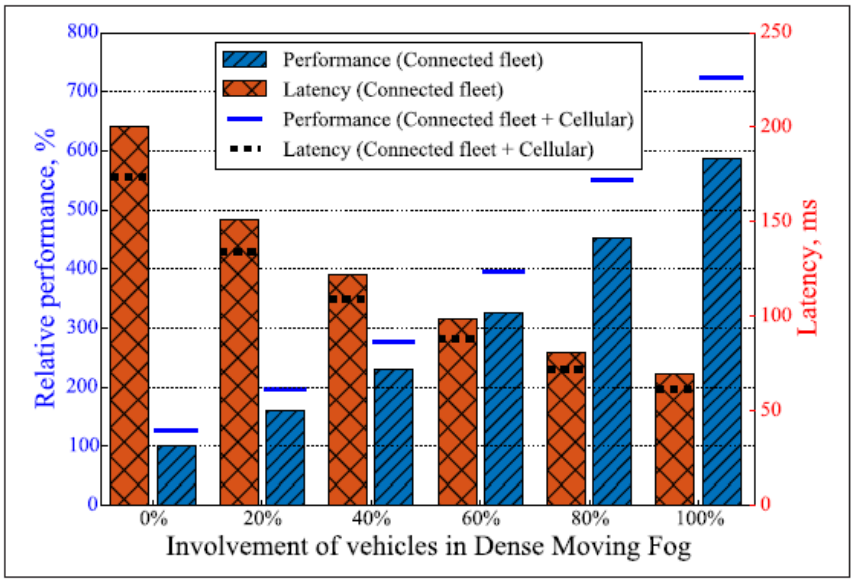

Figure (5): Impact of dense moving fog on collaborative data processing.

References:

1. What is fog computing. By Brien Posey | Sharon Shea, Executive Editor | Ivy Wigmore, Content Editor. Last updated October, 2021:

   https://www.techtarget.com/iotagenda/definition/fog-computing-fogging

2. Fog Computing as Privacy Enabler. By Frank Pallas, Philip Raschke, David Bermbach – TU Berlin, ECDF. Published in IEEE Internet Computing (Volume: 24, Issue: 4, July-Aug 2020):

   https://arxiv.org/ftp/arxiv/papers/1910/1910.04032.pdf

   https://ieeexplore.ieee.org/document/9034092

3. Fog Computing: Characteristics and Challenges. By Shabnam Kumari, Surender Singh and Radha. Published in International Journal of Emerging Trends & Technology in Computer Science (Volume: 6, Issue: 2, March-April 2017):

   https://www.ijettcs.org/Volume6Issue2/IJETTCS-2017-04-01-37.pdf

   https://www.ijettcs.org/pabstract.php?vol=Volume6Issue2&pid=IJETTCS-4-01-37

4. Dense Moving Fog for Intelligent IoT: Key Challenges and Opportunities. By Sergey Andreev, Vitaly Petrov, Kaibin Huang, Maria A. Lema, and Mischa Dohler. Published in IEEE Communications Magazine (Volume: 57, Issue: 5, May 2019):

   https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8648449

   https://ieeexplore.ieee.org/document/8648449