International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-9, Issue-6, November 2021
https://doi.org/10.55524/ijircst.2021.9.6.35
Article ID IRPS12045, Pages 153-157
www.ijircst.org

A Review of Research Opportunities in Fog and IoT

Pankaj Saraswat[1], and Swapnil Raj[2]

SOEIT, Sanskriti University, Mathura, Uttar Pradesh, India
Correspondence should be addressed to Pankaj Saraswat; pankajsaraswat.cse@sanskriti.edu.in

ABSTRACT- Within cloud-to-things gamut, Fog is an embryonic design for storing data, performing computations, controlling applications that allocates many of such facilities to the end users. It is applicable to both wireline and mobile situations, spans software as well as hardware, sits on the edge of network as well as among end users and across access networks, and encompasses control as well as data planes. The review spots most noteworthy applications of fog computing. It supports an increasing number of applications as an architecture that includes fifth-generation (5G) wireless systems, Internet of Things (IoT), and integrated artificial intelligence (AI). The possibilities and problems of fog are summarized in this survey study, which focuses mainly on the networking environment of IoT. Fog is importance edge's stems from the conventional cloud's inadequacies as well as the development of new possibilities for the IoT, 5G, and embedded AI.

KEYWORDS- Edge computing, Edge networking, Fog computing, Fog networking, Internet of Things (IoT).

I. INTRODUCTION

Along the various available cloud-to-things continuum, Fog basically is a structural design that distributes the computing, communications, controls, and storage facilities to the end users. Even though the fog is wider than the usual concept of edges, the terms "fogs" and "edges" are often used interchangeably [1,2]. Moving processing, management, and data storage to the cloud has been a major development over the last decade. Computing services, network management services, and storage services, in particular, are being decentralized into a centralized datacenters using cellular core networks and mainstay IP networks. Cloud computing, on the other hand, is now facing increasing difficulties in fulfilling a slew of new needs in the Internet of Things (IoT) [3]. Simultaneously, the number and variety of powerful end-user, network edge, and access devices that includes mobile phones, tablet devices, smart home devices, edge access points, smart cars, smart meters, intelligent buildings controllers, and industrial control systems, has increased. Many types of drones, the robots being used in industries or homes, data conveying lighting systems, button-sized or tiny radio frequency (RF) tuners, and computers on a stick are just a few of the smart edge devices on the way.

As a result, it's now possible and fascinating to question, "Is it possible for your vehicle to serve as your main data storage device?", "Is it possible for a single device in your home to combine the many services and applications offered by distinct systems such as home media centers, set-top boxes of TVs, network routers, and also the energy management box?", "What if smartphones could undertake network controlling tasks that usually are now carried out using different types of gateways in the LTE core network?", "What can a dispersed and immersive network on the edge achieve with a swarm of adjacent smart network edge and endpoints devices?", "Is it possible for device to provide very low latency to upkeep the applications that are delay-sensitive like data analytics on the edge in real-time, streaming data mining, and control functions in industrial applications?". The pendulum between distribution and centralization has been swinging for past many decades, with different kinds of distribution that includes a local leveraging proximity and an end-to-end principle, wherein the principle is exemplified by peer-to-peer (P2P) multicast overlay TCP and congestion control, and the proximity is same as in sensor and Ethernet networks. Fog encapsulates and accelerates this click-to-brick swing back from both perspectives, and for both the data and control planes.

This article begins by describing the wide variety of new problems that the developing Internet of Things presents, as well as the difficulty of addressing such challenging problems using latest computer paradigms. Additionally, many services require AI to be incorporated so as to achieve the required elegance. It then goes on to explain why we'll require a novel architecture—fog for computing, networking, storage, and control, and how it may bridge technological gaps while also opening up new economic possibilities. Choosing who does what and how to "glue" them back together is what architecture is all about. Developers are still in search of architectural principles that aids in numerous evolving software and systems including cyber systems, IoT system, and embedded artificial intelligence systems, in contrast to extra developed technological fields that includes a digital or serial computation or communication and the internet, where robust architectural foundations have been laid (AI). The

authors have to make basic choices about where to perform computation and save the computed data within the cloud gamut, as well as how to transfer computing jobs onto a competent and variably accessible node. The architectural foundation of fog offers path to investigate the discussed model or architecture, and the article focuses on IoT as a comprehensive and wide-ranging application domain above the architectural foundation of the fog.

II. LITERATURE REVIEW

Bangui et al. offer a foglet as a middleware that uses fuzzy similarity and to simplify the evaluation and choosing of services in an environment based on fog or cloud [4]. Then, using a numerical example, we illustrate the selection process before concluding with a sketch of future possibilities.

Fatima et al. provide a thorough review of fog computing's concept, design, and potentials in comparison to cloud computing [2]. The results of state-of-the-art surveys released in 2017 and 2018 are given to help readers understand current developments. Furthermore, this study emphasizes the most important fog computing applications and evaluates twelve newly suggested works for smart metropolises, intelligently managed transportation systems, health care using AI and fog, and hypermedia applications. Finally, the difficulties of fog computing are explored, as well as future research prospects.

Marina refers to smart things as smart cars, smart homes, smart cities, and so on [5]. Technology advances at a breakneck pace around us. More and more affordable and compact gadgets are becoming accessible. These devices differ in various ways, such as size, computing power, and operating mode, and are all connected to a network for data transmission and communication. They build a sophisticated infrastructure known as the Internet of Things when they are combined (IoT). The massive volumes of IoT data generated provide major processing and analytical problems. They provided an overview of IoT trends, problems, and possibilities, and served as a jumping off point for our study in this area. They are concentrating on the incorporation of Cloud computing with IoT, particularly the expansion of traditional Cloud computing to Edge and Fog computing.

Shanker et al. look at the Fog Computing research difficulties [6]. 'Fog computing,' also known as 'edge computing,' is a type of computing that takes place at the edge of a network. Fog nodes are the infrastructure that offers services at the network's edge. The Internet of Things (IoT) operates by hosting applications in a guest operating system (GOS) that runs in a hypervisor directly on the Connected Grid Router (CGR). Other comparable concepts are Mobile-Edge Computing (MEC) and Cloud Computing. They have a lot in common when compared with fog computing technologies or methods. The time utilized by the system to process the data should not exceed more than fifteen milliseconds, as this would degrade the user experience. Fog servers can provide dynamically configurable optimization based on client devices and network circumstances. The fog computing approach may be used to analyze enormous amounts of data produced by IoT applications. When a new technology is introduced, it should be given an appropriate name and recognized by the community. Fog has a lot of characteristics that clouds don't have. Managing or the handling of millions and billions of different devices linked to internet or local networking setup in order to deploy network function virtualization since more or less networking functionalities can only be performed by software. Services and networks that return to the surface in the fog can be installed on demand in an edge device. Fog computing is a situation in which a large number of diverse, ubiquitous, and decentralized devices interact and possibly cooperate with one another, processing tasks without requiring any third-party association. These everyday jobs usually requires supplementary supportive fundamental networking activities over and above any new apps or services development for use in a sandboxed environment. This study will stimulate a lot of research in the field of fog computing applications.

III. DISCUSSION

A. New IoT Challenges Need a New Architecture

The emergence of the Internet of Things brings with it a slew of new problems that can't be properly handled by today's latest and current cloud computing or hosting paradigms. The authors goes through a few of these basic issues here.

B. Stringent Latency Requirements

The systems used in smart grids, industrial manufacturing, gas and oil plants almost all of them requires point-to-point latencies between the edge having the sensor node and the edge having the control node to be less than fifteen to twenty milliseconds. There are further more additional IoT applications, such as communication between the vehicles and communication amongst vehicles and roadside amenities, virtual reality, control system of a drone and high-end game playing, might need latencies of few milliseconds or even lesser. These needs are considerably above the capabilities of most cloud services.

C. Network Bandwidth Constraints

Data is being generated at an exponential pace by the large and quickly increasing number of linked objects. For example, a connected vehicle may generate huge number of data usually in gigabytes almost each and every second. The data contains information regarding the vehicle mobility details including routes followed and speed maintained during the trip; 2) the car's operational circumstances that includes component’s deterioration; 3) films captured by the safety cameras installed in the car; and 4) the surroundings of the vehicle, including such roads and weather situations. A self-driving car will produce much more data, likely to be around one gigabit every moment. The smart grid in the United States is projected to produce petabytes of information each and every year. In 2010, the US Library of Congress produced almost more than 2.4 PB of data every month, the giant search engine Google trafficked approximately one PB per month, and the research laboratory AT&T's network used over 200 PB per year.

D. Resource-Constrained Devices

Many IoT devices will be extremely resource constrained. Sensors, data collectors, actuators, controllers, surveillance cameras, vehicles, trains, drones, and medical equipment implanted in patients are all examples of embedded devices. There are number of resource-constrained systems and devices that will certainly be unable to meet all of the required computational requirements simply with their own restricted resources. Requiring them all to connect directly with the cloud is impractical and costly, since such collaborations over and over again necessitate resource-intensive handling and complicated procedures. For example, a contemporary vehicle's many microcomputers need to update the firmware within them, on the other hand forcing each of the resource-constrained systems to execute intensive secured and cryptographic procedures and complex processes necessary to get firmware updates is unfeasible.

E. Cyber-Physical Systems

These systems are controlled using highly secured algorithms. As more systems are getting connected with internet, the interactions and close integrations between cyber systems and physical systems are becoming increasingly important as in cyber-physical systems, the software and physical components are intensely entangled in order to bring new business priorities and operational requirements [7]. Smart cities, linked vehicles and trains are all examples of cyber-physical systems. The continuous and safe functioning of such systems is often the primary concern. Because taking a system down for any reason may result in substantial company loss or unbearable customer annoyance, there is a requirement of high level of planning in advance.

F. Intermittent Cloud Connectivity

Devices with inconsistent network connectivity to the cloud will have difficulties receiving uninterrupted cloud services. Vehicles, drones, and oil rigs are examples of such equipment. The rig of oil in middle of the marine, outlying away from land generally have solitary satellite communiqué routes to link with the cloud system. The satellites may have wildly changing quality and be unavailable at times. Collecting and analyzing the data and controlling the oil rig, on the other hand, must be accessible even if the rig lacks any network connection with the cloud. For instance, when a vehicle travels through a region where Internet connection is lost, numerous services and apps for the gadgets and people in the car must remain accessible. When a vehicle collapses somewhere and requires one of the control unit or ECU changed in order to operate again, the replacement unit must be verified so as to avoid illegal and possibly malware infested control units from getting fitted. Cloud-based authentication services, on the other hand, will not be accessible in this situation.

G. Challenges in Security

Prevailing Internet cyber security solutions have mainly focused on perimeter-based safeguards, with the goal of safeguarding corporate networks, data centers, and consumer devices. A system or a single item under security is usually put behind a firewall operating in tandem with a system for detecting and preventing intrusion to keep the malware or any kind of threats out of the protected boundaries [8]. Many of the security tasks that generally are resource-intensive are transferred to the cloud too possibly via web services available. Prevailing cloud-based security continues to concentrate on perimeter-based protection that includes sending electronic mails and traffic of the websites to clouds for detecting the threat and authentication and authorization processing.

H. Arrival of New Fog Era

Filling and satisfying the technological gap in IoT support need an innovative and novel design, namely a fog, which spreads processing, controlling, data storing, and network related operations nearby the devices of end users. Fog and cloud work together to create a gamut amid the cloud and endpoints by delivering mutually the advantageous and the inter-reliant services that enable processing, storage, control, and communication anywhere alongside the gamut. Table 1 shows the key features of fog and how it works in conjunction with cloud.

Table 1: Illustrates the Fog's main characteristics and how it works with clouds [9]

	Cloud	Fog
Location and Model of Computing	Centralized in a small number of big data centers.	Often distributed in many locations, potentially over large geographical areas, closer to users along the Cloud-to-Thing continuum. Distributed Fog nodes and systems can be controlled in centralized or distributed manners.
Size	Cloud data centers are very large in size, each typically contain tens of thousands of servers.	A Fog in each location can be small (e.g., one single fog node in a manufacturing plant or onboard a vehicle) or as large as required to meet customer demands. A large number of small Fog nodes may be used to form a large Fog system.
Deployment	Require sophisticated deployment planning.	While some Fog deployments will require careful deployment planning, Fog will enable ad-hoc deployment with no or minimal planning.
Operation	Operate in facilities and environments selected and fully controlled by Cloud operators. Operated and maintained by technical expert teams. Operated by large companies.	May operate in environments that are primarily determined by customers or their requirements. A Fog system may not be controlled or managed by anyone and may not be operated by technical experts. Fog operation may require no or little human intervention. May be operated by large and small companies, depending on size.
Applications	Support predominately, if not only, cyber-domain applications. Typically support applications that can tolerate round-trip delays in the order of a few seconds or longer.	Can support both cyber-domain and cyber-physical systems and applications. Can support significantly more time-critical applications that require latencies below tens of milliseconds or even lower.

I. Research Challenges And Open Questions

As is characteristic of any emerging field of study and development, many of the topics in fog are developed versions of cumulative changes over the last decade or two, as follows.

- In contrast with MANET, fog will be built on far more authoritative, varied, and frequently used edge devices, apps, and endwise categorized nodes enabled by wireless or wired broadband networks.
- In comparison to P2P networks in the mid-2000s, fog encompasses network assessment, network monitoring, service facilitation, as well as management and measurement of network, and service enablement.
- Compared to previous edge-networking work, fog enhances a whole innovative sense of complexity to next level concept to continuously improve the edges, the end devices will work collaboratively to allow greater level of assistance along the cloud-to-things gamut by collectively monitoring and evaluating the rest of the network.

For instance, how to deconstruct and recompose computing workloads among a collection of heterogeneously competent and variably accessible fog nodes that are wirelessly linked and constrained by bandwidth and energy. Following that, we'll go through a few different types of fog research problems.

Fog may be utilized to assist edge networking (10). Fog, for example, can help network edge devices and end-user devices (e.g., vehicles, drones, industrial and consumer robots, smartphones, and virtual reality gaggles) form local networks by providing temporary security credentials and acting as local application servers and data storage servers for the edge ne. Some fog functionalities for edge networking support may be implemented on end-user devices. In such situations, understanding how fog functions interact with end-user device operating systems and hardware is critical.

Fog introduces additional security concerns. Generally speaking, the non-centralized systems are much more susceptible to assaults than any of the centralized ones as centralized system are less prone to such assaults. While cloud works in highly secured facilities chosen and managed by operators of the cloud system, fog often has to function in extra risky environs—where they can best fulfill the demands of a customer and often where users want them to be. The edge devices will be considerably smaller than clouds (for example, a fog node on a vehicle, a manufacturing facility, or an oil rig), and therefore will not have as many resources to defend themselves as clouds. Additionally, any fog system may lack the global information required to identify threats.

Fog's closeness to the handlers and location on the edge, on the other hand, allows it to assist in addressing some emerging IoT security issues, as described in the preceding sections. Fog can, for example, serve as the first nodes for access control and traffic encryption, apart from providing isolation and contextual integrity.

IV. CONCLUSION

Fog is beginning to alter the future landscape of a number of sectors, fostering innovation across the whole industrial food chain, including the following.

- Operators of networks.
- End-to-end service providers.
- Suppliers of network equipment.
- Integrators of systems.
- Cloud computing service providers.
- Manufacturers of cutting-edge technology.
- Manufacturers of computer chips.

The pendulum has swung toward "click" during the last 15 years. It has now begun to fluctuate back nearer to "brick," indicating that fog and cloud coexist. Fog is helpful for instantaneous dispensation, fast innovation, user-centric

service, and edge resource pooling, whereas cloud will be useful for huge storage, heavy-duty computing, global coordination, and wide-area connection. 2016 is an exciting year to begin methodically investigating what fog could look like in the next 15 years, as well as the differences it will bring to networking and computing.

REFERENCES

[1]. Aazam M, Zeadally S, Harras KA. Offloading in fog computing for IoT: Review, enabling technologies, and research opportunities. Futur Gener Comput Syst. 2018;

[2]. Haouari F, Faraj R, Alja'Am JM. Fog Computing Potentials, Applications, and Challenges. In: 2018 International Conference on Computer and Applications, ICCA 2018. 2018.

[3]. Zhao YS, Chao HC. A green and secure iot framework for intelligent buildings based on fog computing. J Internet Technol. 2018;

[4]. Bangui H, Rakrak S, Raghay S, Buhnova B. Moving towards smart cities: A selection of middleware for fog-to-cloud services. Appl Sci. 2018;

[5]. Tropmann-Frick M. Internet of things: Trends, challenges and opportunities. In: Communications in Computer and Information Science. 2018.

[6]. Kruba Shanker D. Fog Computing: Synergizing Cloud, Big Data and IoT-Strengths, Weaknesses, Opportunities and Threats (SWOT) Analysis. Int Res J Eng Technol. 2016;

[7]. Sood SK, Mahajan I. Fog-cloud based cyber-physical system for distinguishing, detecting and preventing mosquito borne diseases. Futur Gener Comput Syst. 2018;

[8]. Shekhar Rendla C, Gangadharan GR, Wankar R. Real-World Applications and Research Challenges of Fog/Edge Services. In: Proceedings of the International Conference on Inventive Communication and Computational Technologies, ICICCT 2018. 2018.

[9]. Chiang M, Zhang T. Fog and IoT: An Overview of Research Opportunities. IEEE Internet of Things Journal. 2016.

[10]. Sharma PK, Chen MY, Park JH. A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT. IEEE Access. 2018;