Interplay, Issues and Challenges of Cloud and Fog Computing

Hiba Shakeel
Department of Computer Science and Engineering,Institute of Technology and Management, Aligarh, India
Sushil Kumar Sharma
Department of Computer Science and Engineering,Institute of Technology and Management, Aligarh, India

Abstract

Cloud Computing (CC) and Fog computing (FC) are trending technologies, as everyday voluminous data and IoT devices are being added to the internet.CC provides shared resources to the users, over the internet on a pay-as-you-use and demand basis. The fog paradigm fulfills real-time requests that are received from smart or IoT devices. As the cloud involves remote servers, while fog processes requests near to/on the devices themselves, they along with owning unique characteristics, face various issues and challenges, typically related to privacy, security and performance. This paper gives a clear picture of the cloud and fog paradigm, separately and together. Cloud-fog interplay and the differences between them are also discussed. The paper goes on to highlight various issues and challenges of cloud and fog, after which it concludes.

Keywords. Cloud Computing, Fog Computing, Internet of Things (IOT), Security and Privacy, Smart device

1. INTRODUCTION

Cloud and fog architecture have computing devices that handle miscellaneous user requests. It has rippled through almost every field such as business, healthcare and has mixed their territories. In a world full of IoT devices, where data on the internet changes overtime, cloud and fog have a significant role to play. Cloud and fog, in sync, provide a variety of computational assets to fulfill dynamic user requests. The aforesaid architecture uses virtualization, which provides virtual devices to satisfy multiple clients' demands at once. Cloud overlay fog, where fog handles dire requests so that lesser data reaches the cloud and latency is reduced. With the advent of smart technologies like smart healthcare systems, smart cities, smart devices, pressure on the cloud and fog to handle requests along with needed Quality of Service (QoS) is increasing rapidly.

1.1 Cloud Computing

CC provides internet-based computing services to the users where shared resources like servers, VMs, memory, network, are provided as per the need. Clients do not physically purchase these resources. Hence, the cloud has enabled handling of everything over the internet, from development to modification of applications, where clients only pay for the services they take. Cloud has a pool of resources that provides availability and flexibility to users. Cloud has five essential characteristics, three service models, and four deployment models according to NIST [1, 2].

1.1.1 Characteristic features of Cloud Computing

- *On-demand services*: The client can avail services and resources online which are handled automatically, without any human intervention.
- *Broad network access*: With it as main pillar, services are productively utilized. Light and heavy devices of various configurations get quality services anytime and anywhere.
- *Rapid Elasticity*: It is one of distinguishing features of cloud. It makes sure that resources can be scaled up and down, without trading off QoS.
- *Measured services*: Implementing a metered capability enables the cloud to measure and administer resource usage depending on the type of service.
- *Resource pooling*: Cloud is pool of physical and virtual resources (platform, VMs, etc.) thatprovides multi tenancy. Users cannot precisely tell the physical location of devices.

1.1.2 Cloud Service Models

There are three types of cloud service models [1, 2, 3].

- *Infrastructure as a service (IaaS)*: The service provider (SP) gives the entire infrastructure to the client, on their demand, through the internet. Infrastructure may include software, bandwidth, memory, processor, VMs, etc. Client doesn't control and maintain the infrastructure, it is taken care of by the SP instead. It reduces capital cost. Google, Rackspace, Amazon web services are some example of IaaS.

- *Platform as a service (PaaS)*: SP whichis the host, offers platform, including various softwares and hardware to the clients. It facilitates development of applications, with the help of tools that the SP gives. Window Azure, Google App Engine are PaaS examples.
- *Software as a Service (SaaS)*: SP offers softwares, which run on cloud infrastructure, over the internet. Clients need not to install or execute the application on their devices. Email services is most common example. IBM, Oracle are examples of such SP.

1.1.3 Cloud Deployment Models

There are four cloud deployment models [1, 2]based on scale, access to resources and authority.

- *Public*: It is the most widely used deployment model and provides public services for the general mass. Same data or services are given by SP to all clients, which are open to all. They are mostly unpaid. Facebook, LinkedIn, Google are examples.
- *Private*: Services and resources are for asingleorganization and utilized by many users at a time. It gives good security, privacy and a private environment to client information,hence private cloud is costlier than the public. It is hosted by the organization or a third party.
- *Community*: Resources are used by several organizationsthat share a common goal (e.g. security). It can be hosted both internally and externally. Management is done either by the organization or by some third party. Cost lies in between of public and private cloud.
- *Hybrid*: Hybrid cloud is fusion of public, private and community cloud, offering more flexibility. Each entity is unique. Critical jobs are performed using private cloud, as they offer more security. While non-critical jobs are done through public. It provides cost satisfaction along with security features of private but more management is required.

1.2 Fog Computing

FC is an extension technology of CC.IoT-enabled devices send enumerable requests to cloud,which add plenteous data to network. This consequently raises issues like security and privacy threats, congestion and low QoS.Fog is positioned between cloud and IoT devices. Heterogeneous fog nodes scattered at different geo-locations collaborate to form a network, to store and process data at network edge[4]. Fog addresses requests of IoT devices' quickly and more securely than cloud. The requests are handled by fog nodes, so that cloud is not repeatedly pursued and lesser data reaches it. Features of fog, highlighted by NIST [4] that makes it a standout among peer paradigms are:

1.2.1 Characteristic features of Fog Computing

- *Location awareness and Low latency*: As fog nodes are closely located to IoT devices, processing, storage, management and fulfilment of request is done rapidly when compared to CC. Hence, better QoS are attained at network edge.
- *Large number of nodes*: Addressing of foglets require large number of dispersed fog nodes, to provide faster service in close vicinity to the data source.
- *Mobility support*: When a device moves from one physical location to other, fog services are unhindered because fog application module is transferred from one node to other. It thus provides location-based mobility to users without halting the services.
- *Wireless networks*: Wireless sensors in IoT use distributed services of fog. Fog complements IoT, as low power and energy is wasted to facilitate scalability and mobility.
- *Real-time request handling*: Real-time information is important for IoT, sofog does not process requests batch-wise.
- *Heterogeneity*: As fog is responsible for handling different types of requests arriving from heterogeneous smart devices, it itself should be heterogeneous.
- *Linkage to cloud*: Many requests need both cloud and fog for being processed. Quick handling is done at fog. Fog uses cloud for heavy processing of requests and data.

- *Big sensor network*: Large number of sensors forming big networks are used by fog monitoring IoT-related environments like Smart Grid.
- *Geo-distribution*: The nodes are geographically distributed, in order to satisfy users timely and support mobility.
- *Interoperability and federation*: Most fog services are real-time, for which various SP should collaborate. Thus, fog services and components must be joined at various levels.

2. CLOUD-FOG COMPUTING ENVIRONMENT

Cloud and fog have a complex interplay. They often work in synchronization, forming a complete architecture, along with IoT. Figure 1 shows cloud, fog and IoT system [4]. The complete architecture has three layers/ tiers viz. IoTdevice layer, fog layer and finally the cloud layer [5].

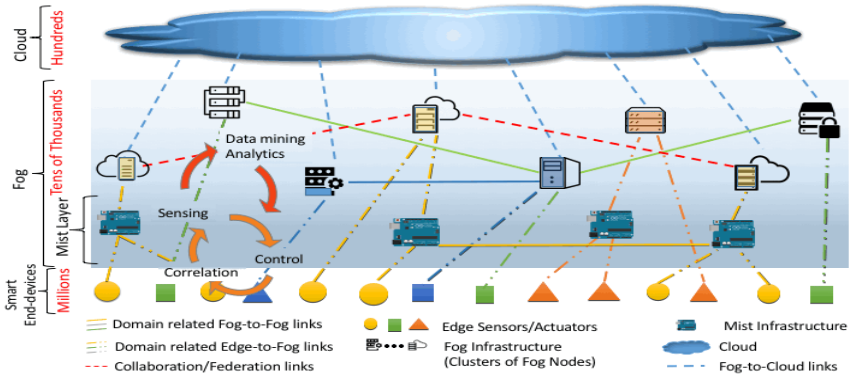

Figure 1. Cloud, Fog, and IoT System

2.1 Interdependency of Cloud and Fog Computing

Fog assists cloud and cloud assists fog. Fog is used for localization, while cloud provides global centralization[6]. FC is heterogeneous in nature. IoT devices like smart TV, smart traffic light send requests to fog nodes [7]. These fog nodes are expected to service requests urgently. The computational capacity of fog node is limited, in comparison to cloud. Fog nodes with their full processing and storage capacity, service the requests instantly. Once the services are handled, the resultant information is sent to cloud, to be analyzed and stored. Some requests may need heavy processing and storage capacity, which fog node may fail to provide. In such scenario, requests are further transmitted to the cloud. Cloud does the needful processing.

Cloud and fog consolidate each other in fulfilling users' requests, adding benefits of both the technologies. Cloud gives additional computing and storing facility to fog, to handle massive requests. On the other hand, fog reduces the amount of information and service demands that reach cloud. Fog also adds features like reduced latency and bandwidth, increased mobility, which makes it a suited choice for IoT. Hence, they both have their own roles and cannot replace one another.

2.2 Cloud Computing Vs Fog Computing

Both thetechnologies use VMs but are as much different from each other as much they are similar. The major differences between them is due to differences in the underlying hardware. Cloud has datacenters with huge capacities, while fog nodes include gateways, fog devices and fog servers, with relatively very little computational power. Higher availability with high energy consumption is provided by cloud ,whereas moderate availability with lesser energy consumption is provided by fog [8]. Also, cloud is not a good fit for services that need urgent actions by server. Table 1 marks the key differences between CC and FC [9].

Table 1. Key Differences between Cloud and Fog Computing [9]

S. No	Parameter of Comparison	Cloud Computing	Fog Computing
1	Architecture	Centralized	Decentralized

2	Latency	Very high (May take a week)	Very low (Will take few minutes at maximum)
3	Mobility	Lesser support to mobility	Total support
4	Security	Inferior to fog	Better than cloud
5	Coverage	Global	Local
6	Data storage duration	For a very long time (Even for years)	Very short time (Maximum few weeks)
7	Privacy Control	Inferior to fog	Better than cloud
8	Nodes	Few	Large number
9	Proximity to users	Multiple hop	Single hop
10	Hardware	Powerful datacenters	Relatively week fog nodes
11	Operating cost	Relatively high	Relatively low
12	Energy used	High	Low
13	Location awareness	Absent	Present
14	Vulnerability	High	Low
15	Real-time service	Supported	Highly supported
16	Last mile connectivity	Leased line	Wireless

3. ISSUES AND CHALLENGES OF CLOUD COMPUTING

Some of the important cloud issues and challenges are [10-13]:

- *Security and privacy*: Security and privacy are biggest challenges of CC. CC provides services using remote servers, on which clients' softwares and data run. Hence, cloud data is susceptible to security threats like data stealing, loss, data leak, data tampering.
- *Technical issues*: Various technical issues arise due to heavy load and requirement for high-speed internet connectivity, which makes the cloud system complex.
- *Data lock-in*: Standard APIs, if not present, hamper migration of services and applications among clouds. Data portability, migration, and vendor lock-in problems may occur.
- *Data segregation*: During multi-tenancy, when VMs are located near to each other on same server or hard disk, issues related to separating memory of users may rise.
- *Data location*: For data and information safety of the users, geographical location of data plays an important role. Rules for data varies with countries and data types. Client may get involved in legal issues without even knowing.
- *Recovery and back-up***:** Data recovery is as important as data security in cloud. Cloud must facilitate recovery of data. Data recovery process gets slower in case of disaster.
- *Cost*: Often, one of the computation, communication and integration cost suffers at the hands of other. When cloud client moves from one model to other, migration cost adds, while infrastructure cost reduces. This is more of a problem in the hybrid cloud, as in hybrid model, distribution of data is in between private, public and community clouds.
- *Service Level Agreement (SLA) related challenges*:Customer must be sure of fulfillment of various factors related to service delivery like quality, reliability, confidentiality. SLAs provide such guarantees. SLAs are written in view of meeting all client's requirements. Achieving SLA becomes a challenge when a business is moved from one model to another, as different clouds require different meta-specifications.
- *Migration related issues*: According to the survey of IDC, 2008, when organizational data migrates from one cloud to another, security and privacy issues rise. It is difficult to move from IaaS to SaaS, as only few functions are moved out, while core activities are kept in-house.
- *Anticipated and unanticipated workloads*: Processors, memory and network are virtual resources which utilize very less power than traditional datacenters. Large workloads (predictable/unpredictable) are submitted to VMs [19]. Loads may vary overtime.
- *Heterogeneous and homogeneous workloads*: Workloads maybe heterogeneous (dissimilar e.g., in terms of execution time, hardware requirement) or homogeneous (similar). Hence, cloud should be in such a way that different types of workloads should be handled by it.
- *Batch and transaction workload*: Workloads maybe of batch or transaction types. Transaction workload unlike batch, requires input from user, time to time e.g.online transactional system. Batch workloads are non-preemptive while

transaction workload is preemptive. Batch workload fluctuates but transactional workloads do not. Hence, depending upon the workload type, a suitable scheduling algorithm must be used.

- *Flexibility*: Cloud flexibility refers to its ability to handle dynamic change in resource requirements. As time increases, demand of the resources may grow, these demands must be automatically perceived by the cloud and should be accommodated. A cloud should have an efficient resource management facility.
- *Maximizing resources and minimizing cost*: Cloud should provide maximum resource utilization with least cost. Also, unhindered services should be given to clients.
- *Migration of VMs*: Migration of VMs from one host to the other, helps coping with the issue of insufficient resources. So, VM migration should be facilitated by cloud.
- *Reducing energy consumption*:Due to large number of computational resources, carbon emission is often very high. Strategies must be applied to reduce it.
- *Executing Long Running Jobs*: Some requests of cloud may require longer processing without being interrupted or failing. Cloud should employ strategies and techniques for unavailability and failure detection, in order to migrate workload to available computing resources. This should be done with minimum latency, so that interruption of services is not felt at client's end.

4. ISSUES AND CHALLENGES OF FOG COMPUTING

A major application of FC is IoT [7]. Fog's issues and challenges must be identified and resolved to utilize real time services. Several issues and challenges of cloud enabled fog are [14- 18] :

- *Performance Issue*: Performance issue is major issue of fog, as quoted by CISCO. Fog must provide good performance with good QoS, particularly in terms of latency to IoT devices. If services are not met in real time, then the whole idea of fog becomes useless. This can be resolved by using appropriate load balancing or scheduling algorithms.
- *Fog Server Placement*: Each fog server has resources present at different locations of network edge. For proper management, aspects such as range of fog servers, transmission, communication and collaboration between them are considered. Strategies for efficient fog servers' placement must be used to handle location and management of fog server and to give best services to clients.
- *Network Management challenge*: Fog environment has large number of IoT devices and sensors with different configurations such as processing power, memory, OS, etc. Management of heterogeneous smart devices is an important issue. Network security from various attacks like sniffer and jamming attacks must also be taken care of.
- *Resource Management challenge*: Smart devices require large storage and processing power. In cloud-fog system, management of devices at network edge, between cloud and fog and inside cloud must be done altogether. It becomes more challenging due to heterogeneous devices. Efficient management of the environment givesgood quality services.
- *Security Challenges*: The continuous transmission of data between smart devices and fog nodes may lead to critical security issues. So, various security measures must be taken. Security is less in fog as compared to cloud, due to distributed nodes. Cloud security and privacy mechanisms cannot be used for fog. Fog security and authentication must be developed and included.
- *Privacy /Data Leak Issues*: Primary issue of fog-IoT paradigm is privacy. Fog nodes, which are near to users, has more critical information in comparison to cloud. Various privacy algorithms are implemented between cloud and fog to overcome this issue.
- *Decentralized Data Allocation*: Unlike cloud, data processing in fog is done in fog nodes, which minimizes time. Hence, it reduces latency as servers are not overloaded. However, decentralized process leads to issues like different execution environments.
- *Mobility Management*: With the presence of network connection, fog nodes and IoT devices can move in any environment. However, mobility of IoT devices and fog nodes may break services and reduce quality. Hence, their mobility must be managed.
- *Design of Multi-objective Fog environment***:** Fog must be designed in a way that it meets various objectives (latency, power consumption, etc.) to fully utilize nodes and provide multi-level services.
- *Fog Hardware***:** Fog does not efficiently utilize the underlying hardware like routers, base stations, access points, storage devices, Wi-Fi, optical networks, gateways, hence development of specialized hardware for fog are much required.
- *Offloading of fog nodes*: A node can offload task to nearby nodesto reduce processing latency. So, fog load balancing must be intelligently implemented.
- *Malicious Attacks*: Due to distributed location, fog nodes face threat of various attacks. Existing mechanisms are not efficient in detecting attacks; therefore, innovations are needed for malicious attack proof fog paradigm.

- *Scalable Design of Fog Schemes*: Existing algorithms do not go well with exponential increase in IoT devices, hence newer or improved strategies must be implemented.
- *Access Control Management*: Measures to achieve access control are must for system security. Likewise, access control measures should be developed for fog.
- *Energy Consumption*: Fog nodes use lot of energy due to processing at network edge and promise of good QoS. Energy saving hardware, strategies and policies should be developed for cloud and fog.
- *Authentication Issues*: Authentication of fog service shareholders (cloud SP, internet SP and users) is a serious issue as fog has distributed nature. Algorithms for real-time authentication must be developed.
- *Energy aware & adaptive Fog storage*: Such storage technique not only brings user and data closer but also provides additional functions like energy saving.
- *Coupled resource management in Fog:* Cyber physical systems (CPS) with cloud features called sensor-based cloud computing can improve performance in terms of speed. Combined resource management may lead to service failure.
- *Fog based intelligent transportation system*: Intelligent transportation system (ITS) are gaining popularity for traffic system in 5G network of big data analytics. ITS devices are connected to cloud for processing using IoT. However, cloud generates massive data that ITS application can't handle. To deal with this, fog instead of cloud, is given data processing to provide speedy response and save bandwidth of network.

5. CONCLUSION

Based on the above study, it is right to say that FC is an add-on to CC. Fog is a technological breakthrough, which very well suits IoT environment. Cloud provides various services to IoT devices but with fog, QoS can be enhanced. Cloud is centralized in nature, while fog enables processing at network edge. Both cloud and fog have some peculiar characteristics which make them suitable for different environments. However, both have some issues and challenges that must be curtailed. Security and privacy are recognized as major issues of cloud, as performance is for fog.

6. FUTURE WORK

Future work includes optimization of performance of cloud and fog, considering different quality parameters.Strategies that consider improvement of performance, security and privacy must be developed to make cloud-fog system more robust. Design of multi-objective algorithms for cloud and fog environment must be focused on.

7. REFERENCES

[1] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

[2] Piplode, R., & Singh, U. K. (2012). An overview and study of security issues & challenges in cloud computing. *International Journal of Advanced Research in Computer Science and Software Engineering, ISSN, 2277*.

[3] Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2008). A break in the clouds: towards a cloud definition. *ACM sigcomm computer communication review*, *39*(1), pp. 50-55.

[4] Iorga, M., Feldman, L., Barton, R., Martin, M., Goren, N., & Mahmoudi, C. (2017). *The nist definition of fog computing* (No. NIST Special Publication (SP) 800-191 (Draft)). National Institute of Standards and Technology.

[5] Alzoubi, Y. I., Al-Ahmad, A., & Jaradat, A. (2021). Fog computing security and privacy issues, open challenges, and blockchain solution: An overview. *International Journal of Electrical & Computer Engineering (2088-8708)*, *11*(6).

[6] Wang, Y., Uehara, T., & Sasaki, R. (2015, July). Fog computing: Issues and challenges in security and forensics. In *2015 IEEE 39th annual computer software and applications conference 3*, pp. 53-59. IEEE.

[7] Stojmenovic, I., & Wen, S. (2014, September). The fog computing paradigm: Scenarios and security issues. In *2014 federated conference on computer science and information systems*, pp. 1-8. IEEE.

[8] Jalali, F., Hinton, K., Ayre, R., Alpcan, T., & Tucker, R. S. (2016). Fog computing may help to save energy in cloud computing. *IEEE Journal on Selected Areas in Communications*, *34*(5), pp.1728-1739.

[9] Firdhous, M., Ghazali, O., & Hassan, S. (2014). Fog computing: Will it be the future of cloud computing?.

[10] Sadim, M., & Sharma, R. K. Issues in Cloud Storage Technique and Future Direction.

[11] Daryapurkar, J. U., & Bagde, K. G. (2014). Cloud computing: Issues and challenges. *International Journal on Recent and Innovation Trends in Computing and Communication*, *2*(4), pp. 770-773

[12] Saharan, K. P., & Kumar, A. (2015). Fog in comparison to cloud: A survey. *International Journal of Computer Applications*, *122*(3).

[13] Kandukuri, B. R., & Rakshit, A. (2009, September). Cloud security issues. In *2009 IEEE International Conference on Services Computing*, pp. 517-520. IEEE.

[14] Yi, S., Hao, Z., Qin, Z., & Li, Q. (2015, November). Fog computing: Platform and applications. In *2015 Third IEEE workshop on hot topics in web systems and technologies (HotWeb)* pp. 73-78. IEEE.

[15] Yi, S., Qin, Z., & Li, Q. (2015, August). Security and privacy issues of fog computing: A survey. In *International conference on wireless algorithms, systems, and applications*, pp. 685-695. Springer, Cham.

[16] Sajid, M., & Raza, Z. (2013, December). Cloud computing: Issues & challenges. In *International Conference on Cloud, Big Data and Trust 20*(13), pp. 13-15.

[17] Taneja, M., & Davy, A. (2016). Resource aware placement of data analytics platform in fog computing. *Procedia Computer Science*, *97*, pp. 153-156.

[18] Atlam, H. F., Walters, R. J., & Wills, G. B. (2018). Fog computing and the internet of things: A review. *big data and cognitive computing*, *2*(2), 10.

[19] Alam, M., Haidri, R. A., Mahek & Yadav, D. K. "Efficient task scheduling on virtual machine in cloud computing environment," International Journal of Pervasive Computing and Communications *17*(3), pp. 271-287, 2022.

Biographies

Hiba Shakeel received her bachelor's and master's degree in Computer Science and Applicationsfrom Aligarh Muslim University, Aligarh, India in the year 2017 and 2020 respectively.Her research interest areas include Load balancing, Cloud computing and Fog Computing.

Sushil Kumar Sharma received his MCA and M.Tech degree from GLA College, Mathura, India in the year 2005 and 2012 respectively. He holds 15 years of teaching experience and is Assistant Professor at Institute of Technology and Management, Aligarh, India. His research interest areas include Big Data and Cloud Computing.