Research Article Available online www.ijsrr.org ISSN: 2279–0543

International Journal of Scientific Research and Reviews

Edge Computing: Network and Security Challenges

Narayanan Subbiah[1*] and R.Saranya[2]

[1,2] Department of Information Technology, SRM Valliammai Engineering College, kancheepuram 603202, TamilNadu, India.

ABSTRACT

Internet of Things (IoT) connects physical objects in real world to the internet and transmitting huge amount of information to the cloud data center to process. The centralized cloud processing center on collected data faces various problems such as delay in transmission, netwrok bandwidth constraint, network and security issues. As a strategy to alleviate issues in network, bandwidth and security, edge computing has become a new paradigm for addressing the needs of the Internet of Things and localization computing. Well-known cloud computing increases delay in processing, but edge computing migrates data calculations or storage to the edge of the network near the IoT devices. Thus, multiple edge compute nodes distributed across the network can minmize computational issues from a centralized data center and can significantly reduce latency in message exchanges. Besides, the distributed edge architecture balances network traffic and avoids spikes in traffic in the IoT network, reduces delay between edge/cloud servers and end-devices, and reduces response time for real-time IoT applications compared to traditional cloud services. There are still many problems in practical applications that need to be solved, including optimizing edge computing performance, security, interoperability, and intelligent edge operations management services.

KEYWORDS: Edge computinhg, Internet of Things, Network, Security, Cloud computing, Fog Computing.

***Corresponding Author**

Dr.S.Narayanan

Department of Information Technology, SRM Valliammai Engineering College

Kancheepuram-603202,Tamilnadu, India.

Email:nsk1178@gmail.com, Mob No-9962116401

INTRODUCTION

Now a days Cloud computing is the leading technological platform for storing and processing huge amounts of data. It has its spread into all industries. Industries deploy their data to the cloud server instead of keeping it on their local machines. Cloud computing is becoming the overarching Internet approach for information storage,processing, retrieval and management, and IoT devices become the major outlets of service applications. The next generation networks is the successful integration of cloud computing and IoT devices. However, with cloud computing, faces several fundamental challenges:

Bandwith

The rapidly growing number of IoT nodes are produces data at an exponential rate. It is estimated that an autonomous vehicle generates about terabytes data[1]. To support such applications, it is important to keep a high-rate data exchange between cloud and IoT devices. But with the long-thin connection between cloud and end users, the net-work bandwidth becomes a bottleneck for cloud computing[2.]

Latency

Mainstream cloud computing services cannot guarantee latencies because many IoT applications, such as vehicle-to-vehicle communications, require latencies below a few tens of milliseconds[3].

Real-time response

IoT devices real-time response is too latency-sensitive to deploy on cloud computing[4]. With the advent of new tech-nologies like 5G and IoT, traditional cloud computing is failed in addressing problems like high latency, resource allocation, and bandwidth limitation[5].

Edge computing that enables data from IoT nodes to be processed at the nodes itself or near the nodes. The data is processed near the node at a local processor or server and not the main cloud computing data center. All the edge nodes then transmit the received data to the cloud storage center[5].It provides a computing model for edge intelligence computing services. The location where the edge computing occurs is called the edge node, which can be any device between the data generation node and the cloud center that has computing resources and network resources. For example, a sensors is an edge device between a person and a cloud computing center, and a gateway is an edge node between a smart home and a cloud center[6].

ARCHITECTURE OF EDGE COMPUTING

In general, Edge Computing technique is the process of performing computing tasks physically close to data collecting nodes, rather than in the cloud or on the device itself. Over the past decades we've seen different architectural patterns for processing systems. Depending on the bottleneck problem of the system it was designed as a centralized processing or de-centralized processing system. The increaing amount of data from IoT devices and the limitations of the transmitting and networking layer (and computation) currently lead to a de centralized processing system like Edge mpting.

The below picture shows a typical Edge Computing architecture. It is defined by a hierarchy of computing power and latency, both of which are highest on the top level and decreasing downwards. This allows us to perform latency-critical computations as low on the hierarchy as possible and computing intensive calculations as high as necessary.

Cloud

On this top layer of this architecture cloud node compute power and storage are virtually limitless, but latencies and the cost of data transport to this layer can be very high. In an Edge Computing processing application the cloud computing can serve as long-term storage, coordinator of the immediate lower levels or poweorful resource for irregular process.

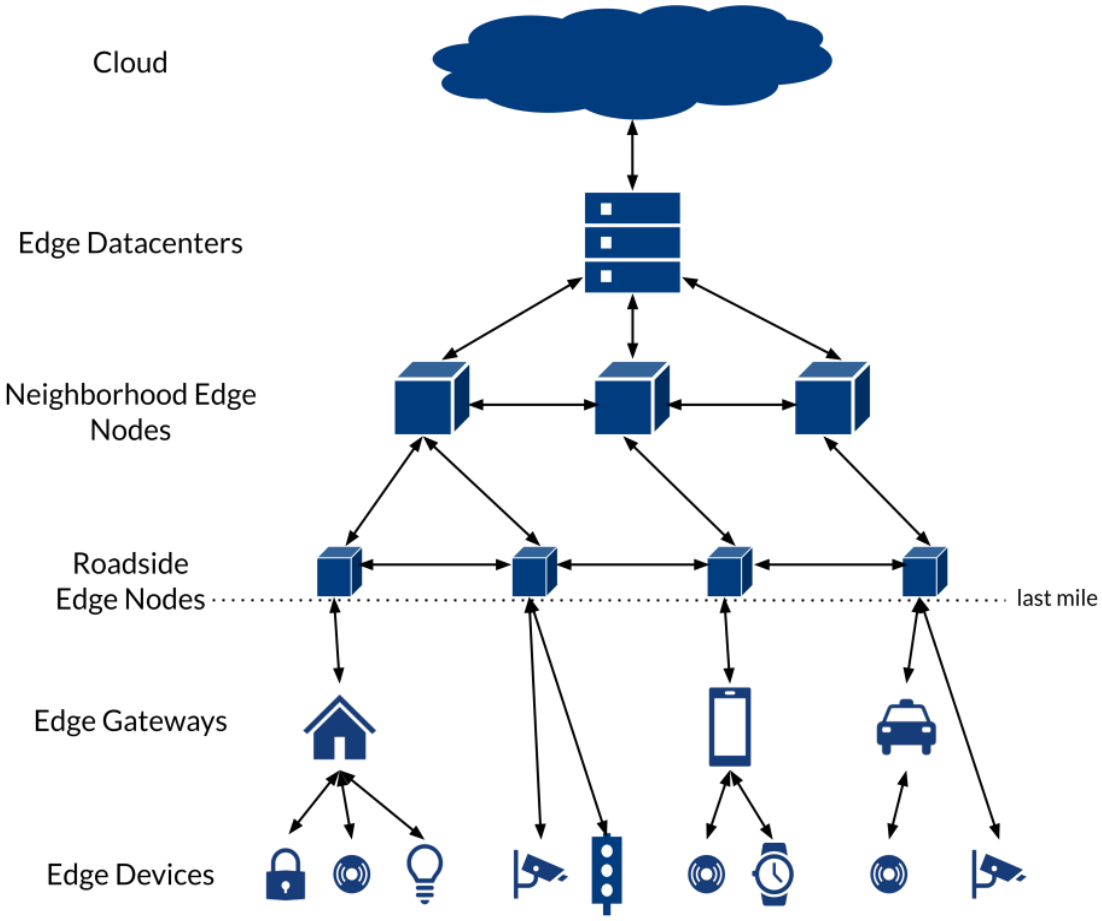

Figure 1. Layers of Edge Computing

Edge Node

These nodes are located near the last mile of the network. Edge Nodes are devices capable of routing to cloud network traffic and usually also possess high compute power. They can range from base stations, routers or switches up to small-scale data computing center.

Edge Gateway

Edge Gateways are similar to network entry point but less powerful. This gateway performs several critical functions from translating protocols to encrypting, **processing**, managing and filtering data. If you imagine an IoT ecosystem, a gateway sits between devices and sensors to communicate with the cloud and can manage computations that do not require specialized hardware such as GPUs

Edge Devices

On this layer small devices with very limited resources such as single sensors or embedded systems are available. These devices are usually used for a single type of computation and often limited in their communication capabilities. Devices on this layer might be smart sensors, traffic lights or environmental sensors.

This nodes enables faster communication between devices in different mists, which are able to communicate through their respective Edge Nodes. It can also further reduce network traffic load and cost by omitting communication over the internet.

POTENTIAL OF EDGE COMPUTING

IoT nodes are quite powerful, capable of gathering, storing, and processing more data than ever before because it uses strong hardware technologies.This provides facilities for industries to optimize their networks and relocate more processing functional nodes closer to where data is gathered at the network edge, where it can be analyzed and applied in real time much closer to intended end users.

Since the data doesn't have to travel all the way back to the central server for the device to know that a function needs to be executed. Edge computing networks can greatly reduce latency, improve the performance, scalability, reliability, throughput and adpdability.

Lattency Reduction

If applications depend on immediate response transmitting data to the cloud, processing and retransmitting the data back to the end user device may take too long. The most important benefit of edge computing node is its ability to increase network performance by reducing latency. Since IoT edge computing nodes process data locally or in nearby edge data nodes, the information they collect doesn't have to travel nearly as far as it would

under a traditional cloud architecture.

Data throughput

Edge nodes may produce enormous amounts of data. By processing data closer to the source and reducing the physical distance it must travel, edge computing can greatly improve the throughout. The end result is higher speeds for end users, with throughout measured in microseconds rather than milliseconds.By performing the necessary computations on Edge Nodes close to the device, most of the path can be pruned. This is especially important when considering the increasing importance of the internet of things and the rising number of devices connected to the internet.

Reliability and robustness

The important functionality of edge node is should still be available, even if communications path to the central cloud are impaired. This can be achieved by relying on local communication with an Edge Node which should be less prone to problems. If an Edge Node fails, the node will be shifted to an alternative Edge Node.

Privacy

Most of the applications collecting user data is required or at least useful. The users' privacy can be preserved by aggregating the data on the Edge Node instead of the cloud if the aggregated data is sufficient.

Scalability

Computing power of node is limited by their size. Developing a new applications that requires stronger hardware for all possible users or the network administrator to update the devices, which limits the use cases' adoption rate. Edge Nodes do not affect fom these problems and can be extended both very easily and continuously. Using a suitable Edge Computing node framework, adding, replacing or updating Edge Nodes is a very simple and highly automated process.

Adaptability

Edge Nodes easily adpting the changes according to circumstances. Edge Nodes can be easily configured to provide individual subsets of functions, depending on the environment. While some applications are only useful in cities, other appilications may be more beneficial in rural areas. Due to the direct connection to the cloud and higher-level Edge Nodes, moving workloads and freeing up computing power for critical applications is possible and can be done on the fly.

EDGE SECURITY CHALLENGES

Fog and edge computing front-end devices may not have sufficient resources to protect themselves from the attacks. Attackers' targets front end devices because in which the attackers are capable of performing a malicious activity at the edge network where the front-end devices are located and the cloud network does not have full control on it Specifically,outdoor-based front-end devices, which rely on the distant cloud to keep them updated with the security software. Furthermore, the attacker may also damage or control the front-end device and send false data to the cloud.security challenges exist around the processing and storage at the edge node. New strategic plans need to be developed to improve security beyond traditional cloud data center security practices to include heterogeneous mobile and Internet of Things (IoT) computing security.

Distrubuted attack

In Edge computing data is highly distributed.Data for one application alone can be distributed across hundreds of sites or nodes. Edge security measures also need to take into account the huge diversity of edge computing nodes and devices, and a flexible infrastructure needs to be developed that adapts as needed within manageable guidelines[8,9,10].

A physical threat

Edge cmputing locations are more prone to physical tampering and theft. Remote edge locations typically have no IT staff, so this must further be factored into security and management strategy. This makes multiple layers of security even more important, such as encryption and multi-factor authentication.

Connectivity and security challenges

Connectivity will not be constant because some edge devices may be in movement.Security mechanisms need to continue to provide security even if the edge system is disconnected from the management console, whether intermittently or for consistent periods. Companies not allowing direct connections between edge devices and the cloud to reduce risks.Security practices need to be implemented differently in different edge layers along the edge continuum. Separate specific methods can be adopted within each tier in order to factor in important differences in the compute footprint, deployment scale and connectivity reliability, along with physical and network security challenges.The three main tiers within the edge[8,9,10.]

Upper tier

This top tier refers to top layer of the edge computing closer to cloud computing secure data centers. It's security tools in these kinds of settings are largely the same as those used in the cloud computing data center. However, some advanced of method is necessary due to the smaller scale and to support the coordination of Kubernetes clusters distributed across edge data center locations.

Middle tier

This middle tier contains components situated outside secure data computing centers, yet still able to support virtualization and/or containerization. Smart Nodes Edge IoT and compute resources can usually sup-

port robust security features[15].

Lower tier

This tier nodes uses microcontroller and micro processor that are highly distributed, such as sensors or actuators that perform little or no localized compute - more abilty nodes designed to ad-dress time and safety-critical applications.Limited capacity nodes Edge resources often depend on upstream more capable devices for additional security measures.

Cloud computing server's framework and centralized data storage is vulnerable to many security threats. which restricts its development so Its security has emerged as important issues. On the other hand fog and edge is considered as more secure architecture because the data that is collected is momentarily stored and evaluated on local fog or edge nodes nearest to data source, thus decreasing the dependency and complexity on the internet. This storing, processing exchanging and analyzing the data locally makes it hard for network attackers or hackers to gain access to the data. During processing on data in fog or edge there is no real time exchange of data between the cloud and the devices, thus, it becomes very difficult for eavesdrop attackers to perceive the personal data of any user.Since fog or edge computing inherits many features of cloud computing so does it inherits risks also. It is not fully secured.Following are the security threats in edge and fog computing:

Deceive

By generating fake information the network attackers imitate their identities to deceive other enti-ties. It can also damage the network performance by consuming more energy, storage area and network bandwidth due to the fake data packet.

Tampering

In edge or fog computing to degrade and disrupt the execution performance and efficiency of fog computing, network attackers either modify or delays or drops or delete the data that is being transmitted. Most of the time, this kind of attack is difficult to detect because the end user's mobility and the condition of wireless network may cause delay and failure in the transmission.

Spam

Attackers flooding unnecessary data including fake data, redundant values and information. Spam consumes vital network resources.

Sybil

The network criminals convert the genuine nodes into compromised nodes using fake name and identities to control the fog computing effectiveness. It generates fake reports as the results prepared by these reports are not worth trusting and also can expose the personal information of a legitimate user.

Jamming

Large amount of data packets inserted into the transmission channels or its resources in order to restrict

or jam the genuine user from having an efficient and reliable network access.

Eavesdropping

Control of the transmission channel take over by attackers to read or listen the transmission contents without the users' consent. Vulnerability of the data encryption technique is used by attacker.

Denial of Service

These intrusion attacks consume large volume of network resources like bandwidth, battery, time thus degrading the performance of fog as the fog resources are limited.This is achived by attackers sending fake data towards fog and edge nodes and floods them with large number of fake requests to make them unavailable for their legitimate users

Collusion

Group of attackers collude eachother to mislead the genuine groups or acquire legal advantages. To strenthening the attack two or more groups can collude to attack a group of edge nodes or fog nodes or IoT nodes with clouds or fog nodes with IoT nodes.

Man-in-the-Middle

A temporary scenario created by network attackers to stand in between the communicating nodes to relay their data exchange or modify this communication data without disclosing this to the users as they feel they are exchanging the data with each other directly.

Impersonation

A network attacker behaves like a true server and offers fake or malicious services to the end user by creating an impression of being true fog nodes or servers.

Privacy

It is a serious issue in fog or edge computing because user’s data is collected, processed, transmitted and shared over fog or edge nodes. Disclosure of privacy information is under threats or attacks is oblivious. The user's privacy includes the following four aspects:

Identity Privacy

A user identity includes the basic attributes of an entity and these identi-ties are vulnerable to get exposed for getting authentication of fog or edge nodes by providing all this information.

Data Privacy

During communication on fog or edge nodes the user data may get exposed to an untrusted party and different types of vital information can be obtained.

Usage privacy

The usage privacy normally means the sequence with which the user uses the services of the fog or edge. For instance, the smart meter reading may reveal the users sleeping time or the time when they are not home, thus violating the privacy of the user.

Location privacy

In the modern navigation, location based service, most of the mobile applications use users current or saved location. Thus in order to enjoy internet services the users have to sacrifice the location privacy. But the location privacy is extremely important to be kept secured as it can be used by the attackers to determine the trajectory of the user.

NETWORKING CHALLENGES IN A FEDERATED EDGE ENVIRONMENT

The edge computing facilitates distributed computing due to dynamic networking environment and constantly varying demands at the end-user level. The network architecture will need to ensure that the Qulaity of service of deployed applications and services are not affected[18]. For this, the quality of user experience cannot be compromised and the coordination of activities to facilitate edge computing must be seamless and hidden from the end user[19].Edge computing faces the following challenges in network.

User mobility

Mobile user continuously roaming to different place so keeping track of different mobility patterns very big challenge mechanisms for application layer handover.

Dynamic Environment

When dynamic movement is increased latency is also increased which is intolerant to some real time services, Dynamic state of the network leads to decrease of quality of service

Uninterrupted.

The long distance between cloud and the front-end IoT devices can face issues derived from the unstable and intermittent network connectivity. For example, a CIoT-based connected vehicle will be unable to function properly due to the disconnection occurred at the intermediate node between the vehicle and the distant cloud.

Resource-constrained

Commonly, many front-end devices are resource-constrained in which they are unable to perform complex computational tasks and hence, CIoT systems usually require front-end devices to continuously stream their data to the cloud. However, such a design is impractical in many devices that operate with battery power because the end-to-end data transmission via the Internet can still consume a lot of energy.

A Service-Centric Model

The traditional host-centric model the server is established in a given geographic location which is restrictive in a number of ways[20]. In service centric model model, services may have a unique identifier, may be replicated in multiple regions, and may be coordinated. However, this is not a inconsiderable task, given the current edge design of the Internet and protocol stacks, which do not facilitate global coordination of services.

Reliability and Service Mobility

The dynamic movement of user devices and edge nodes may connect and disconnect from the Internet instantly.This could potentially result in an unreliable environment. A casual end-user device will be expecting seamless service perhaps via a plug-and-play functionality to obtain services from the edge, but an unreliable and dynamic network could result in latencies.

Multiple Administrative Domains

The edge and fog network infrastructure will need to be able to keep track of recent status of the network, edge servers and services deployed over them. When a collection of end-user devices requires a service at the edge, first the potential edge host will need to be determined.The most feasible edge node will then be chosen as the resource for the execution.In order to achieve a global view of the network and maintain synchronization across separate administrative domains, the network orchestrator will need to follow a centralized structure. However, the control operations for coordinating the internal operations of a private domain will need to be distributed. In other words, the control of the network should be distributed over the network but should be placed within a logically centralized context.

CONCLUSION

This paper review the challenges in security and network in edge and fog computing.The researches can follow the challenges to solve the probem.Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion..

REFERENCES

1. M. Chiang and T. Zhang, “Fog and iot: An overview of research opportunities,” IEEE Internet of Things Journal,2016. 3(6):854–864.
2. P. Hu, S. Dhelim, H. Ning, and T. Qiu, “Survey on fog computing: architecture, key technologies, applications and open issues,” Journal of Network and Computer Applications.2017,98: 27–42.
3. T. H. Luan, L. Gao, Z. Li, Y. Xiang, G. Wei, and L. Sun, “Fog computing: Focusing on mobile users at the edge,” arXiv preprint arXiv:1502.01815, 2015.
4. S. Yi, Z. Hao, Z. Qin, and Q. Li, “Fog computing: Platform and applications,” in 2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb). IEEE, 2015:73–78.
5. Weishong Shi, Jie Cao, Quan Zhang, Youhuizi Li, and Lanyu Xu “Edge Computing: Vision and Challenges” *IEEE Internet of Things Journal* 2016:3(5): 637-646
6. Rimal B P, Van D P, Maier M. Cloudlet Enhanced Fiber-Wireless Access Networks for Mobile-Edge Computing [J]. IEEE Transactions on Wireless Communications, 2017, 1-1.

7. L. M. Vaquero and L. Rodero-Merino, “Finding your way in the fog:Towards a comprehensive definition of fog computing,” ACM SIGCOMM Computer Communication Review,2014 44(5):27–32.
8. J. Shropshire, “Extending the cloud with fog: Security challenges & opportunities,” 2014.
9. T. S. Dybedokken, “Trust management in fog computing,” Master’s thesis, NTNU, 2017.
10. K. Saharan and A. Kumar, “Fog in comparison to cloud: A survey,” International Journal of Computer Applications2015 : 122(3)
11. S. M. H. Ashjaei and M. Bengtsson, “Enhancing smart maintenance management using fog computing technology,” in 2017 International Conference on Industrial Engineering and Engineering Management IEEM, 10 Dec 2017.
12. F. A. Kraemer, A. E. Braten, N. Tamkittikhun, and D. Palma, “Fog computing in healthcare–a review and discussion,” IEEE Access,2017:5 9206–9222.
13. T. V. N. Rao, A. Khan, M. Maschendra, and M. K. Kumar, “A paradigm shift from cloud to fog computing,” International Journal of Science,Engineering and Computer Technology 2015,5(22):385
14. K. Kai, W. Cong, and L. Tao, “Fog computing for vehicular ad-hoc networks: paradigms, scenarios, and issues,” the journal of China Universities of Posts and Telecommunications, 2016,23(2):56–96.
15. M. Aazam and E.-N. Huh, “Fog computing: The cloud-iotn/ioe middleware paradigm,” IEEE Potentials2016,35(3):40–44.
16. Abdullah Aljumah and Tariq Ahamed Ahanger “Fog Computing and Security Issues: A review” “2018 7th International Conference on Computers Communications and Control (ICCCC)
17. S. Yi, C. Li, and Q. Li. A survey of fog computing: Concepts, applications and issues. In *Proceedings of the Workshop on Mobile Big Data*. Hangzhou, 2015.
18. L. M. Vaquero and L. Rodero-Merino. Finding your way in the fog: Towards a comprehensive definition of fog computing. *SIGCOMM Computer Communication Review*,2014, 44(5): 27–32.
19. I. Stojmenovic, S. Wen, X. Huang, and H. Luan. An overview of fog computing and its security issues, *Concurrency and Computation: Practice and Experience*,2015, 28(10): 2991–3005.
20. A. C. Baktir, A. Ozgovde, and C. Ersoy. Enabling service-centric networks for cloudlets using SDN. in *Proceedings of the 15th International Symposium on Integrated Network and Service Management*, Lisbon, Portugal,May 8–12, 2017.