International Journal of Engineering & Technology, 7 (2.7) (2018) 92-95

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Survey on secure protocols for data sharing through edge of cloud assisted internet of things

K Sai Prasanthi [1]*, K.V.Daya Sagar [2]

[1]Research Scholar, Department of Computer Science and Engineering, K L E F deemed to be University,
[2]Associate Professor, Dept. of Electronics and Computer Science Engineering, K L E F deemed to be University,
**Email: prasanthi1216@kluniversity.in*

Abstract

Nowadays Internet of Things (IoT) is the trending topic where we go. IoT is included in almost every device surrounded by us where valuable information is shared over the network to store it in the cloud or to transfer as a message alert to an individual. IoT devices generate a huge amount of data but only caring information is required and for that analytics needs to be performed. Analytics are reaching outside of the traditional datacenter towards the edge, where the IoT data is generated. So, here in this paper, the importance of secure data sharing over a network, generated by IoT devices is described and along with that the data flow between IoT and edge server is discussed, and the requirement of edge analytics is focused.

Keywords: *cloud computing; edge computing; internet of things; cryptography; analytics*

1. Introduction

Internet of Things (IoT) is a system of associated physical gadgets that are to be had via the internet. The 'element' in IoT could be a man or a vehicle with constructed- in-sensors, i.e. devices that have been allocated an IP deal with and may accumulate and trade statistics over a network without manual assist or intervention. The embedded innovation inside the gadgets encourages them to talk with inner states or the outer situation, which thus impacts the picks taken. IOT is the idea of essentially connecting any tool with an on and off switch to the Internet. This carries the whole thing from mobile telephones, espresso makers, garments washers, earphones, lights, wearable devices and nearly something else we will consider. This moreover applies to components of machines, as an example, a jet engine of an aircraft or the penetrate of an oil rig. As distinct, within the occasion that has an on and off transfer at that point possibilities are it is able to be a chunk of the IoT. The professional company Gartner says that with the aid of 2020 and there could be more than 26 billion related gadgets. The upside is that we are able to do things we never imagined. But as with every top issue, there's a disadvantage to IoT: It is becoming a more and more appealing goal for cybercriminals. We must not neglect that IoT is a big machine of connected "things" which likewise carries individuals. The relationship can be among human individuals, people-things, and things-things. Actually, the IoT considers for all intents and functions with unlimited open doorways and associations that manifest, a giant quantity of which we cannot consider or completely understand the impact of these days. It definitely opens the manner to a ton of chances but similarly to many difficulties. Security is a major problem that is regularly raised.

In October 2016 the world received a harsh wake-up call about the importance of IoT security. A catastrophic distributed denial-of-service (DDoS) attack that created a massive Internet outage for millions of users on the east coast of the United States. The attack disrupted many popular websites such as Netflix, Twitter, and PayPal. An investigation revealed that the method behind the hack involved infecting thousands of connected devices with unchanged default passwords. Routers, surveillance cameras and other IoT devices with unchanged default passwords were infected to form a botnet that launched a denial-of-service attack on Dyn, a major internet services provider. The aftermath of the attack highlighted the challenges posed by IoT devices. Engineers have pioneered new 'IoT-aware' Wi-Fi networks, which are designed specifically to accommodate the unique security challenges of IoT devices. Organizations and users face two primary challenges when it comes to secure deployment of IoT devices. They must have the ability to connect to Wi-Fi in a simple manner, given their mass numbers, and then remain secure once connected. Given that adding more security features to a network tends to reduce the simplicity of connecting devices, it can be difficult to achieve both goals simultaneously.

Managing IoT devices can be very tough. Mainly because they sometimes depend heavily on quick data processing. For this to happen, the data centers or servers responsible for processing the IoT device data must be near the IoT device. This is not possible always. Therefore, to avoid this problem and improve the network's efficiency along with the security so that IoT data is processed as quickly as possible, one of the ways is to make use of Edge Computing.

2. Importance of Security in IoT Devices

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

3. Importance of Edge Computing

Edge computing comes in handy especially for healthcare related IoT devices, where the lives of the patients may depend upon the critical data.

In today's world, all the internet connected devices are taking advantage of cloud computing, but the developers and manufacturers of the Internet of Things are discovering the benefits of doing more computing and analytics on the device itself. This on-device approach helps lower the latency for critical applications and makes more independent on the cloud, and effectively manages a large amount of data generated by the IoT devices. An example of this is the recently announced indoor security camera by Nest Cam IQ, which processes when there is a change in the motion of things captured by it, whenever strangers are seen, and send alerts if something is not recognized or the parameters are not satisfied. By performing on-camera processing, Nest minimizes the bandwidth rate, processing taken on the cloud, and also the storage of continual raw streams and sending them over the network to the cloud. In addition, on-device processing improves the rate of sending the alerts which include reducing chances of disturbance, periodic faux alarms.

The propensity to do adduce on IoT device processing and analytics are referred to as "edge computing." Imagine the "edge" as the world of Internet-connected devices and gateways sitting on the field — the peer to the "cloud." Edge computing gives new possible outcomes in IoT applications, especially for devices depending on machine learning for tasks, for example, face recognition, and hindrance evasion.

The rate at which information is prepared is very basic with regards to IoT devices. For instance, because of an IoT device like the smoke indicator, the reaction must be fast. Though for certain other IoT devices, the reaction required need not be that fast.

The ascent of edge computing is an emphasis of a notable innovation revolution that starts with amalgamate processing and afterward develops into more conveyed models.

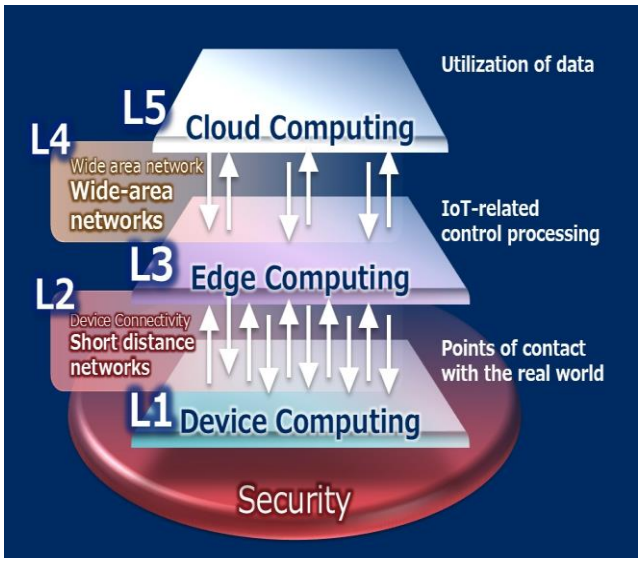


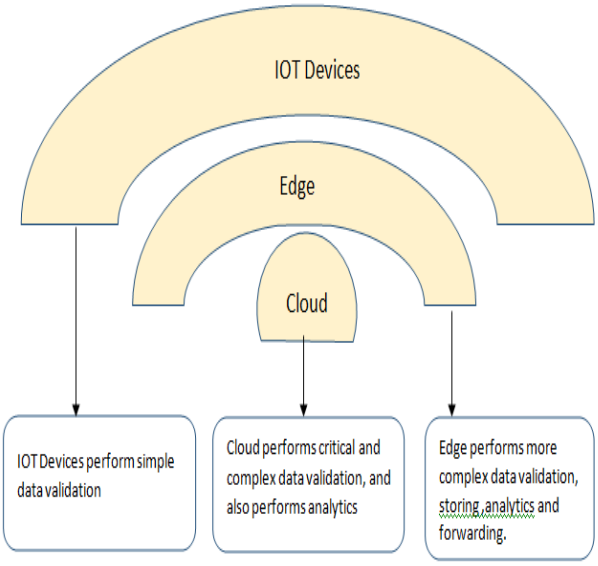
Figure 1: Levels Of Edge Computing

Edge Computing Architecture Figure.1 illustrates the basic architecture of edge computing. Notice that the edge computing servers are closer to the end user than cloud servers. Thus, even though the edge computing servers have less computation power than the cloud servers, they still provide better QoS (Quality of Service) and lower latency to the end users. To study the advantages and disadvantages of edge computing, we will focus on the architectures of both, and compare the two. Obviously, unlike cloud computing, edge computing incorporates edge computation nodes into the network.

4. IoT and The Edge:

In IoT and for some phenomenal applications the design involves the IoT device, edge, and the server. The intention is to scrutinize near the surroundings of the device, for the instant report and instant decision making. This is important for programs using transitional data in algorithms that use machine learning to make realistic and independent decisions. If we send the data to the cloud server back it could proliferate differently the anticipated value.

For example, an industrial IoT application may include sensors in the manufacturing production line or traffic signals. Edge peripherals can capture real-time information to internally process the data by the device itself and utilize the same in preventing from failure, optimizing the production or even diverting the traffic.



5. Edge Analytics

Basically, analysis can be done at the stage where data is being originated. This is about analyzing instantly. So, the architectural design should contemplate the built-in analysis. For example, in traffic lights, the signals should embed sensors that provide intelligent tracking and effective running of traffic such that it is adequately capable to raise an alarm to nearby police departments. Another good example is security cameras. Transmitting the live clipping directly without any change is ineffectual. There are techniques that can detect a change from the previous image to the new one, those changes will only be transmitted. This is helpful and makes more sense such that it is processed at the end of the device instead of sending the data

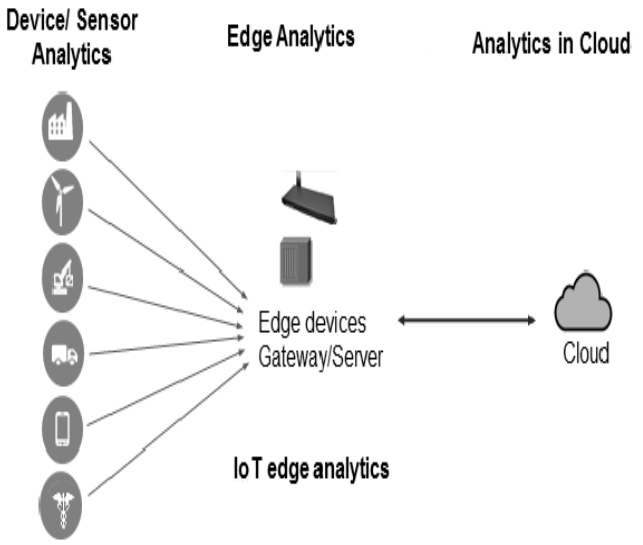


Figure 3: Edge Analytics

over the network to perform the analysis. Now the time has come to understand that edge analytics is important, and it is essential that data generated by the devices need to be analyzed at the device end itself. However, we should understand that in edge analytics only a part of data is analyzed, and the rest of the raw data is discarded adequately. When raw data is discarded there may be important insights that may get missed. So, we should also consider this situation and think whether this loss of data is bearable or not. As we know data is valuable and it should be analyzed to detect patterns and do business analysis.

6. Five Use Cases for Edge Computing and Analytics

6.1. IoT Sensor Information Gathering and Analytics:

An essential objective of sensor analytics is to identify peculiarities. The knowledge that is picked up by looking at deviations from a set up perspective can have numerous utilizations, including anticipating and proactively counteracting equipment failure in a production plant, cautioning a medical caretaker in an electronic emergency unit a patient's blood pressure drops, or permitting a data center administrator to focus on data-driven settlement on information-driven choices about ventilating, heating etc.

6.2. Customer in Retail Sector Analysis

The functionality of IoT within the retail world is tremendous. IoT permits to retailers to interact with the clients to decorate the insave association. Smartphones could be the way for retailers to stay related to their customer's level out of the store. Interfacing thru clever telephones the functionality of IoT inside the retail international is significant. IoT offers a chance to shops to interface with the customers to improve the in-store involvement. Smartphones might be the course for stores to stay associated with their shopper's degree out of the store. Connecting through Smartphones can permit outlets to serve their customers better. They can likewise music clients pattern of shopping thru a store and decorate save layout and vicinity premium objects in excessive rush hour gridlock zones.

6.3. Mobile Data Analysis:

Mobile data, much like IoT sensor information, is being generated with expanding rate, however, the drawback of the greater part of this information is that a few, or even a substantial portion of it, isn't expected to answer information investigation questions. Many organizations are facing difficulties in identifying the information from a large amount of data. Having edge computing and analytics empowers organizations to better comprehend their information and analytics needs to thin Big Data and just process and dissect the data important to the query.

6.4. Compliance Analysis at Financial Sectors:

One important function of data analysis at finance sector is to discover, and stop, non-compliant exchanges. At the point when organizations need to set aside the opportunity to move information back to the central data center or transfer it to a distributed computing design for processing and analyzing, the latency diminishes the importance of the information. Utilizing smaller scale data center in finance-related organizational branches empowers analytics to occur continuously, implying that rebellious or noncomplaint exchanges are gotten and halted substantially more rapidly, which can have a genuine and positive effect on the primary concern.

6.5. Manufacturing and Production Sectors Monitoring and Information Gathering:

IoT is helping mechanical organizations accumulate, store and hand-off information from different manufacturing and production sector.

7. Cloud Computing Vs Edge Computing

Table I summarizes the key features of cloud and edge computing technologies. Cloudlets is proposed to address some challenges to process IoT devices generated data. From the application point of view, security in a multi-vendor edge computing-based ecosystem. The similarities between the two technologies are openness. Operators open their networks to third parties to deploy innovative applications and services.

Table 1: Comparison of Cloud and Edge Computing

	Edge	Cloud
Bandwidth	Cost Is Reduced	Cost Is Increased
Response Time	Less	More
Deployment	Decentralized-Computing	Centralized Computing
Storage	Limited	Unlimited

8. Conclusion:

With the development of IoT, edge computing importance will be raised since data analytics will be done nearby to the end users. Many important things can be accomplished like transmission latency can be minimized to improve response time in real-time IoT applications. Further, it can also reduce the delays caused due to traffic over the network. And moreover, the load of the cloud server will be minimized, and a trivial amount of load could be shared by edge server.

References

[1] Forbes article by Bernard Marr, "Will Analytics on the Edge be the Future of Big Data?", Aug 2016. www.networkworld.com
[2] H. Kumarage, I. Khalil, A. Alabdulatif, Z. Tari, and X. Yi, "Secure Data Analytics for Cloud- Integrated Internet of Things Applications," IEEE Cloud Computing, vol. 3, no. 2, 2016, pp. 46-56
[3] M. Satyanarayanan, P. Simoens, Y. Xiao, P. Pil- lai, Z. Chen, K. Ha, et al., "Edge Analytics in the Internet of Things," IEEE Pervasive Computing, vol. 14, 2015, pp. 24–31.
[4] Forecast: "The Internet of Things, Worldwide, 2013. ", Gartner, 2013.

[5] L.Wang and R.Ranjan, "Processing Distributed Internet of Things Data in Clouds," IEEE Cloud Computing, vol. 2, no. 1, 2015, pp. 76–80.
[6] S. Yi, Z. Hao, Z. Qin, and Q. Li, "Fog Computing: Platform and Applications," 2015 3rd IEEE Workshop Hot Topics Web Systems and Technologies (HotWeb), 2015, pp. 73–78.