International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

FOG COMPUTING

[1]Parinitha J, [2]Mallelala Adarsh

[1]Assistant Professor, Dept. of ECE, SJCIT Chikkaballapur, India
[2]Student, Dept. of ECE, SJCIT Chikkaballapur, India

ABSTRACT:

The Fog computing is not a replacement of cloud it is just extends the cloud computing by providing security in the cloud environment. Similar to Cloud, Fog provides data, compute, storage, and application services to end-users.Cloud computing promises to significantly change the way of use computers and store our personal and business information with these new computing and communication paradigms arise new data security challenges. Existing data protection mechanisms such as Encryption have failed to protect the data in the cloud from unauthorized access. We proposed a different approach for securing data in the cloud using offensive decoy technology. We monitor data access in the cloud and detect abnormal data access patterns.When unauthorized access is suspected and then verified using challenge questions, we launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user's real data. Experiments conducted in a local file setting provide evidence that this approach may provide unprecedented levels of user data security in a Cloud environment

INTRODUCTION

Fog Computing is an extension of Cloud Computing. As in a Cloud, Fog computing. also provides data, compute, storage, and application services to end-users. The difference is Fog provides proximity to its end users through dense geographical distribution and it also O supports mobility. Fog computing improves the Quality of service and also reduces latency.In this framework, each smart thing is attached to one of Fog devices. Fog devices could be interconnected and each of them is linked to the Cloud. As Fog computing is implemented at the edge of the network, it provides low latency, location awareness, and improves quality-of-services (QoS) for streaming and real time applications. Typical examples include industrial automation, transportation and networks of sensors and actuators. The Fog paradigm is well positioned for real time big data analytics, supports densely distributed data collection points, and provides advantages in entertainment, advertising. In this era, Cloud computing is achieving popularity every day. The ease of use and storage which is provided to users for personal and business purposes is increasing its demand. Although, cloud computing provides an environment through which managing and accessing of data becomes easier but it have consequences such as data leakage, data theft, insider attacks etc. Very common risks now days are data theft attacks. The Twitter incident is one example of a data theft attack from the Cloud. Several Twitter corporate and personal documents were ex-filtrated to technological website Tech Crunch and customers' accounts, including the account of U.S. President Barack Obama, were illegally accessed. The attacker. used a Twitter administrator's password to gain access to Twitter's corporate documents, hosted on Google's infrastructure as Google Docs. The damage was significant both for Twitter and for its customers. Ovan Dijk and Juels have shown that fully homomorphic encryption, often acclaimed as the solution to such threats, is not a sufficient data protection mechanism when used alone. To resolve these issues a mechanism which can detect such malicious activities is required. For this, Fog computing is paradigm which monitors the data and helps in detecting an unauthorized access

BLOCKDIAGRAM

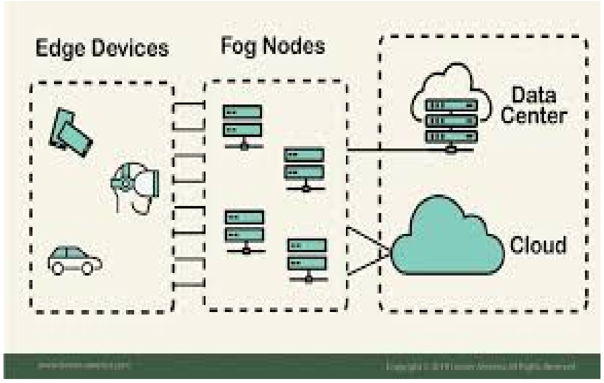

Fig: fog on edge devices

Characteristics of the fog are given below:

a) Low latency and location awareness
b) Wide-spread geographical distribution.
c) Mobility
d) Very large number of nodes.
f) Predominant role of wireless access.
g) Strong presence of streaming and real time application.

The term fog computing, originated by Cisco, refers to an alternative to cloud computing. This approach seizes upon the dual problem of the proliferation of computing devices and the opportunity presented by the data those devices generate by locating certain resources and transactions at the edge of a network.By locating these closer to devices, rather than establishing in-cloud channels for utilization and storage, users aggregate bandwidth at access points such as routers. This in turn reduces the overall need for bandwidth,

Existing data protection mechanisms such as encryption was failed in securing the data from the attack It does not verify whether the user was authorized or not. Cloud computing security does not focus on ways of secure the data from unauthorized access Encryption does not provide much security to our data

We proposed a completely new technique to secure user's data in cloud using user behavior and decoy information technology called as Fog Computing. We use this techniques to provide data security in the cloud. A different approach for securing data in the cloud using offensive decoy technology In 2010 and 2011 Cloud computing security was developed against attackers. Finding of hackers in the cloud. Additionally, it shows that recent research results that might be useful to protect data in the cloudIt does not verify whether the user was authorized or not. Cloud computing security does not focus on ways of secure the data from unauthorized access Encryption does not provide much security to our data. In 2009 we have our own confidential documents in the cloud

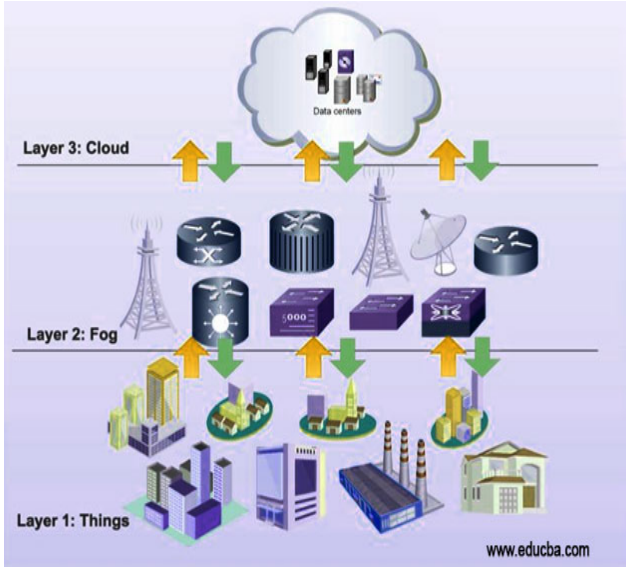

fig .2: architecture of fog computing

The Fog computing architecture consists of physical and logical elements in the form of hardware and software to implement IoT (Internet of Things) network. As shown in figure-2, it is composed of IoT devices, fog nodes, fog aggregation nodes with the help of fog data services, remote cloud storage and local data storage server/cloud. Let us understand fog computing architecture components.

Fog computing architecture

IoT devices: These are devices connected on IoT network using various wired and wireless technologies. These devices produce data regularly in huge amount. There are numerous wireless technologies used in IoT which include Zigbee, Zwave, RFID, 6LoWPAN, HART, NFC, Bluetooth, BLE, NFC, ISA-100.11A etc. IoT protocols used include IPv4, IPv6, MQTT, CoAP, XMPP, AMQP etc.

Fog Nodes: Any device with computing, storage and network connectivity is known as fog node. Multiple fog nodes are spread across larger region to provide support to end devices. Fog nodes are connected using different topologies. The fog nodes are installed at various locations as per different applications such as on floor of a factory, on top of power pole, along side of railway track, in vehicles, on oil rig and so on. Examples of fog nodes are switches, embedded servers, controllers, routers, cameras etc. High sensitive data are processed at these fog nodes.As we know there are three types of data viz. most time sensitive data, less time sensitive data and time-insensitive data. Fog computing architecture works based on type of data it receives. Nearest fog nodes takes data input from the devices. Let us understand working of fog computing architecture.

➡Most time sensitive data are handled by nearest fog node to end device which has generated the data. After the received data is analyzed, decision or action is transmitted to the device. After this, fog node sends and stores summary to cloud for future analysis.

➡Less time sensitive data are sent to aggregate node for analysis. After analysis is performed, aggregate node sends decision or action to the device through nearest node. Aggregate fog node takes seconds or minutes to complete the analysis. The aggregate node later sends the report to cloud for future analysis purpose.

➡The time insensitive data can wait for longer duration (in hours, days or weeks). The data is sent to cloud for storage and future analysis

APPLICATIONS

Connected car: Autonomous vehicle is the new trend taking place on the road. Testl working on software to add automatic steering, enabling literal "hands free" operations of vehicle. Starting out with testing and releasing self-parking features that don't requir person behind the wheel.

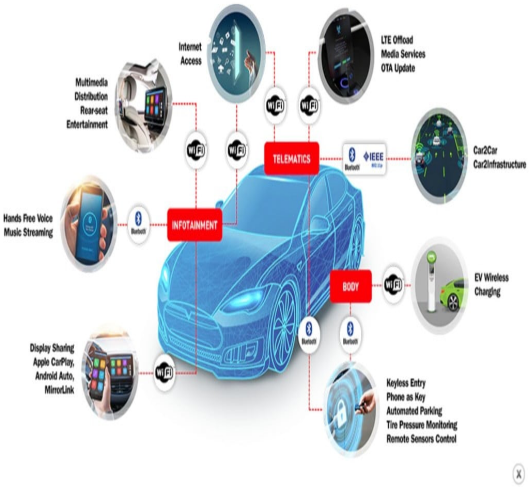

Fig 3: connected car

Smart Grids: Smart grid is another application where fog computing is been used. Based on demand for energy, its obtainability and low cost, these smart devices can switch to other energies like solar and winds. As shown in Figure 5.The edge process the data collected by fog collectors and generate control command to the actuators. The filtered data are consumed locally and the balance to the higher tiers for visualization, real-time reports and transactional analytics.

Smart Traffic lights: Fog enables traffic signals to open lanes on seming flashing lights of the ambulance. It detects presence of pedestrian and hikers, and measures the distance and spend of the close by vehicles, Smart lights serves as fog devices synchronize to send warning signals to the approaching vehicles. The interactions between vehicle and access points are enhanced with WiFi, 3G, mad side units and smart traffic lights Companies involved in developing smart traffic management systems

- Smart Traffic Lights and Connected Vehicles
- IoT and Cyber-physical systems (CPSs

ADAVANTAGES:

- Managing Data Across Platforms
- Improved Co-ordination with Nearby Devices
- Quicker Analysis of Useful Data
- Operating over a Large Geography

CONCLUSION

Fog Computing aims to reduce processing burden of cloud computing. Fog computing is bringing data processing, networking, storage and analytics closer to devices and applications that are working at the network's edge. that's why Fog Computing today's trending technology mostly for IoT

Devices The group has identified numerous IoT use cases that require edge computing including smart buildings, drone-based delivery services, real-time subsurface imaging, traffic congestion management and video surveillance. The group released a fog computing reference architecture in February 2017. Because cloud computing is not viable for many internet-of-things applications, fog computing is often used. Its distributed approach addresses the needs of IoT and industrial IoT, 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.

REFERENCES:

1. Madsen, Henrik, et al. Reliability in the utility computing era: Towards reliable Fog computing Systems, Signals and Image Processing (IWSSIP), 2013 20th International vol. 107, No. 8, Issue August 2019, pp 1474-1481.
2. Zhu, Jiang Improving Web Sites Performance Using Edge Servers in Fog Computing Architecture, Service Oriented System Engineering (SOSE), IEEE. 2013.
3. Sabahi, F. Cloud computing security threats and responses In Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on 2011.pp. 245-249.
4. Stolfo, Salvatore J., Malek Ben Salem, and Angelos D. Keromytis. Fog computing Mitigating insider data theft attacks in the cloud. Security and Privacy Workshops (SPW), 2012 IEEE Symposium on. IEEE, 2012
5. Madsen, Henrik, et al. Reliability in the utility computing era: Towards reliable Fog computing. Systems, Signals and Image Processing (IWSSIP), 2013 20th International Conference on IEEE, 2013
6. C. Wei, Z. Fadlullah, N. Kato, and L. Stojmenovic, On optimally reducing power loss in micro-grids with power storage devices, IEEE Journal of Selected Areas in Communications, 2014 to appear.
7. Bonomi, Flavio, et al. Fog computing and its role in the internet of things. Proceedings of the first edition of the MCC workshop on Mobile cloud computing ACM, 2012, pp. 13-16.
8. Claycomb, W. R., and Nicoll, A. Insider Threats to Cloud Computing: Directions for New Research Challenges, In Computer Software and Applications Conference (COMPSAC), IEEE 36th Annual, July 2012, pp. 387-394.
9. Park, Y, and Stolfo, S. J. Software decoys for insider threat, In Proceedings of the ACM Symposium on Information, Computer and Communications Security, May, 2000 , pp. 93-94.