FOG computing

Jyoti Pawar

Department of Computer Science and Engineering, SVERI's College of Engineering, Pandharpur

Third Year Engineering Student

Abstract:

As we know, 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. Data theft is considered one of the top threats to cloud computing. 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. 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 supports mobility. Access points or set-up boxes are used as end devices to host services at the network. These end devices are also termed as edge network. Fog computing is mainly done for the need of the geographical distribution of resources instead of having a centralized one. A multi-tier architecture is followed in Fog computing platforms.

The term fog computing or edge computing means that rather than hosting and working from centralized cloud, fog system operate on network end. It is term for placing some resources and processes at the edge of cloud, instead of establishing channels for cloud storage and utilization. Fog computing or fog networking is an architecture that uses one or a collaborative multitude of end-user clients or near-user edge devices to carry out a substantial amount of storage (rather than stored primarily in cloud data centers), communication and control, configuration, measurement and management. Fog Networking consists of a control plane and a data plane. For example, on the data plane, fog computing enables computing services reside at the edge of the network as opposed to servers in a data-center. Compared to cloud computing, fog computing emphasizes proximity to end-users and client objectives, dense geographical distribution and local resource pooling, latency reduction.

Fog computing is one approach to dealing with the demands of the ever-increasing number of Internet-connected devices sometimes referred to as the Internet of Things (IoT).In the IoT scenario, a thing is any natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network. Some such things can create a lot of data. Cisco provides the example of a jet engine, which they say can create 10 terabytes (TB) of data about its performance and condition in a half-hour. Transmitting all that data to the cloud and transmitting response data back puts a great deal of demand on bandwidth, requires a considerable amount

of time and can suffer from latency. In a fog computing environment, much of the processing would take place in a router, rather than having to be transmitted.

Fog Computing system is trying to work against the attacker specially malicious insider. Here malicious insider means Insider attacks can be performed by malicious employees at the providers or users site. Malicious insider can access the confidential data of cloud users. A malicious insider can easily obtain passwords, cryptographic keys and files.

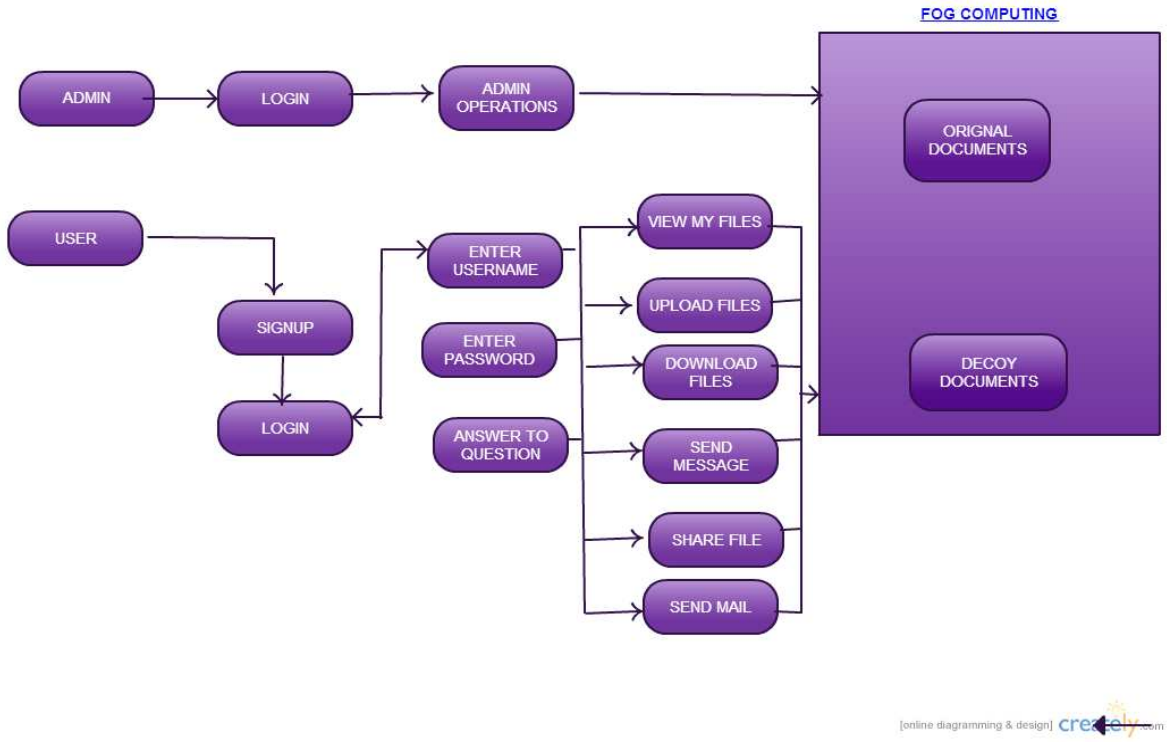

fig.[fog computing architecture]

Securing cloud using Fog

Below is the reference architecture of fog computing environment in an enterprise.You can see that fog network is close to smart devices,data processing is happening closer to devices and the processed information is passed to cloud computing environment.cloud computing has been overtaken by new concept called fog computing which is bigger and better than cloud.The thing that distinguish fog from cloud is just it's mobility,it's proximity to end user and it's dense geographically distribution. In fog computing much of processing takes place in router.this type of computing creates virtual platform that provides networking, compute and storage services between traditional cloud computing data center and end devices. Fog computing has also capability of enabling new breed of aggregated services and application,such as smart energy distribution.In smart energy distribution all the load balancing app will run on network edge devices that will automatically switch to alternative energies like wind and solar.

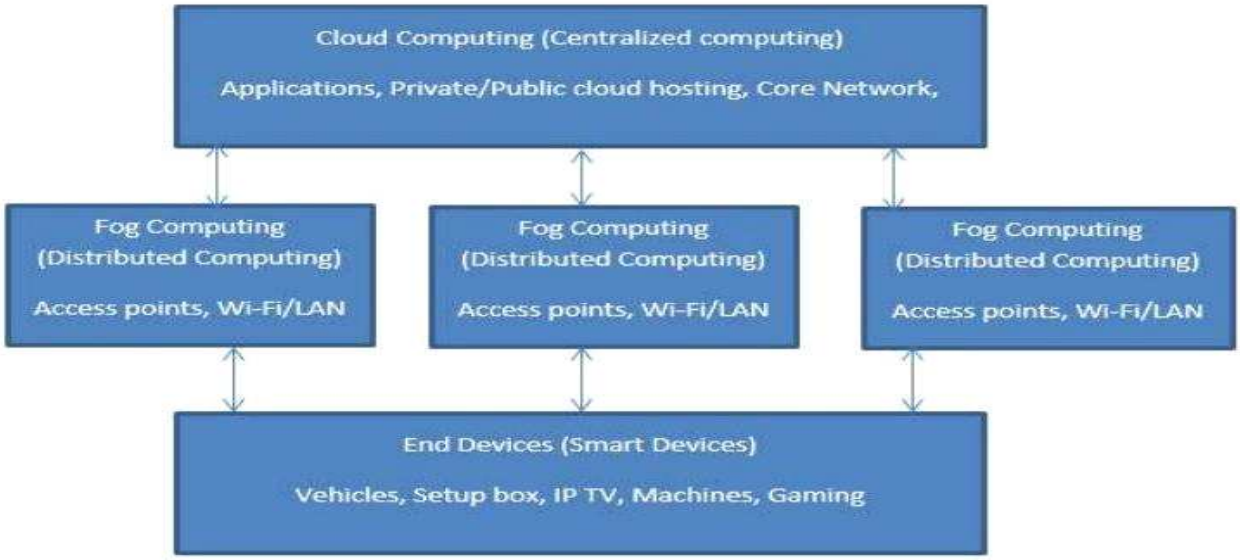

Fig 5: Reference Architecture

Without fog computing:

With fog computing:

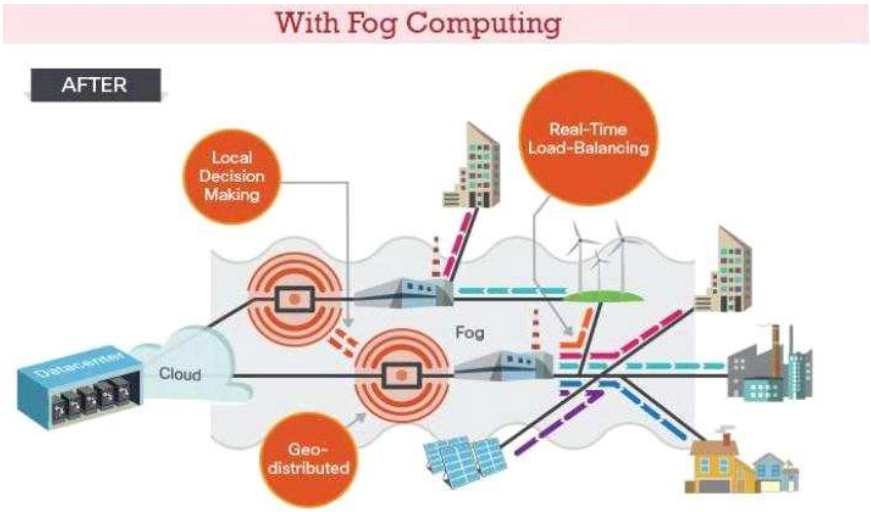

Fig 6 : Without Fog Computing and With Fog Computing in Grid

Example in industry:

Example of fog computing within an industrial context are analytic,optimization and advanced control at a manufacturing work center,unit-operation,across and between unit-operation where sensor and controller,analytical engine will share data interatively in real time.Fog computing reduces bandwidth needs as 80% of all data is needed within the local context such pressure,temperature,material changes,flow rates.

Characteristics of fog computing:

1.Highly distributed concurrent computing system.

2.A peer to peer mesh of computional nodes in virtual hierarchical structure that matches your organization .

3.communication with smart sensor,controller,quality and material control system and others are peers.

4.run on afforadable technology.

5.support multiple platform like unix windows and mac.

6. Built on field-proven high performance distributed computing technologies.

Algorithm Details:

AES (Advanced Encryption Standards):

The Advanced Encryption Standard (AES) is a symmetric-key encryption standard approved by NSA for top secret information and is adopted by the U.S. government. AES is based on a design principle known as a substitution permutation network. The standard comprises three block ciphers: AES-128, AES-192 and AES-256.

Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. AES was selected due to the level of security it offers and its well documented implementation and optimization techniques. Furthermore, AES is very efficient in terms of both time and memory requirements. The block ciphers have high computation intensity and independent workloads (apply the same steps to different blocks of plain text).

Key Length	Number of Rounds
128	10
192	12
256	14

Explanations:

AES is based on a design principle known as a Substitution permutation network. It is fast in both software and hardware. Unlike its predecessor, DES, AES does not use a Feistelnetwork.AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits. The block size has a maximum of 256 bits, but the key size has no theoretical maximum.AES operates on a 4×4 column-major order matrix of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special field. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of cipher text. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

High-level description of the algorithm:

1. Key Expansion: Round keys are derived from the cipher key using Rijndael's key schedule.
2. Initial Round: AddRoundKey: Each byte of the state is combined with the round key using bitwise xor.
3. Rounds:

- SubBytes—a non-linear substitution step were each byte is replaced with another according to alookup table.
- ShiftRows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
- MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
- AddRoundKey Final Round (no MixColumns)
- SubBytes
- ShiftRows
- AddRoundKey

Security Issues in fog computing:

The main security issues are authentication at different levels of gateways as well as (in case of smart grids) at the smart meters installed in the consumer's home. Each smart meter and smart appliance has an IP address. A malicious user can either tamper with its own smart meter, report false readings, or spoof IP addresses. There are some solutions for the authentication problem. The work elaborated public key infrastructure (PKI) based solutions which involve multicast authentication. Some authentication techniques using Diffie-Hellman key exchange have been discussed in Smart meters encrypt the data and send to the Fog device, such as a home-area network (HAN) gateway. HAN then decrypts the data, aggregates the results and then passes them forward. Intrusion detection techniques can also be applied in Fog computing . Intrusion in smart grids can be detected using either a signature-based method in which the patterns of behaviour are observed and checked against an already existing database of possible misbehaviours. Intrusion can also be captured by using an anomaly-based method in which an observed behaviour is compared with expected behaviour to check if there is a deviation. The work develops an algorithm that monitors power flow results and detects anomalies in the input values that could have been modified by attacks.

Intrusion by dynamically generated decoy file:

We placed traps within the file system. The traps are decoy files downloaded from a Fog computing site, an automated service that offers several types of decoy documents such as tax return forms, medical records, credit card statements, e-bay receipts, etc. The decoy files are downloaded by the legitimate user and placed in highly-conspicuous locations that are not likely to cause any interference with the normal user activities on the system. A masquerader, who is not familiar with the file system and its contents, is likely to access these decoy files, if he or she is in search for sensitive information, such as the bait information 126embedded in these decoy files. Therefore, monitoring access to the decoy files should signal masquerade activity on the system. The decoy documents carry a keyed-Hash Message Authentication Code (HMAC), which is hidden in the header section of the document. The HMAC is computed over the file's contents using a key unique to each user. When a decoy document is loaded into memory, we verify whether the document is a decoy document by computing a HMAC based on all the contents of that document. We compare it with HMAC embedded within the document. If the two HMACs match, the document is deemed a decoy and an alert is issued.

Advantages of fog computing

1. Bringing data close to the user - The volume of data being delivered via the cloud creates a direct need to cache data or other services. These services would be located closest to the end-user to improve on latency concerns and data access.

2. Creating dense geographical distribution- Fog computing extends direct cloud services by creating an edge network which sits at numerous points. This, dense, geographically dispersed infrastructure helps in numerous ways. First of all, big data and analytics can be done faster with better results. Then, administrators are able to support location-based mobility demands and not have to traverse the entire WAN. Finally, these edge (Fog) systems would be created in such a way that real-time data analytics become a reality on a truly massive sale.

3. True support for mobility and the IoE- As mentioned earlier, there is a direct increase in the amount of devices and data that we use. Administrators are able to leverage the Fog and control where users are coming in and how they access this information. Not only does this improve user performance, it also helps with security and privacy issues.

APPLICATIONS OF FOG COMPUTING

- **Fog computing in Smart Grid:**

Energy load balancing applications may run on network edge devices, such as smart meters and micro-grids . Based on energy demand, availability and the lowest price, these devices automatically switch to alternative energies like solar and wind.

- **Fog computing in smart traffic lights and connected vehicles:**

Video camera that senses an ambulance flashing lights can automatically change street lights to open lanes for the vehicle to pass through traffic. Smart street lights interact locally with sensors and detect presence of pedestrian and bikers, and measure the distance and speed of approaching vehicles.

- **Wireless Sensor and Actuator Networks:**

Traditional wireless sensor networks fall short in applications that go beyond sensing and tracking, but require actuators to exert physical actions like opening, closing or even carrying sensors. In this scenario, actuators serving as Fog devices can control the measurement process itself, the stability and the oscillatory behaviours by creating a closed-loop system.

- **Decentralized Smart Building Control:**

The applications of this scenario are facilitated by wireless sensors deployed to measure temperature, humidity, or levels of various gases in the building atmosphere. In this case, information can be exchanged among all sensors in a floor, and their readings can be combined to form reliable measurements.The system components may then work together to lower the temperature, inject fresh air or open windows. Air conditioners can remove moisture from the air or increase the humidity. Sensors can also trace and react to movements (e.g, by turning light on or off). Fog devices could be assigned at each floor and could collaborate on higher level of actuation. With Fog computing applied in this scenario, smart buildings can maintain their fabric, external and internal environments to conserve energy, water and other resources.

Software Defined Networks (SDN):

SDN is an emergent computing and networking paradigm, and became one of the most popular topics in IT industry. It separates control and data communication layers. Control is done at a central. SDN concept together with Fog computing will resolve the main issues in vehicular networks, intermittent connectivity, collisions and high packet loss rate, by augmenting vehicle to-vehicle with vehicle-to-infrastructure communications and centralized control.

Conclusion:

With the increase of data theft attacks the security of user data security is becoming a serious issue for cloud service providers for which Fog Computing is a paradigm which helps in monitoring the behavior of the user and providing security to the user's data. In Fog Computing we presenting a new approach for solving the problem of insider data theft attacks in a cloud using dynamically generated decoy files and also saving storage required for maintaining decoy files in the cloud. So by using decoy technique in Fog can minimize insider attacks in cloud.

References:

1. Prevention of Malicious Insider in the Cloud Using Decoy Documents by S. Muqtyar Ahmed, P. Namratha, C. Nagesh.

2. Overview of Attacks on Cloud Computing by Ajey Singh, Dr. Maneesh Shrivastava.

3.www.slideshare.com

4. www.a4academics.com