Survey on Fog Computing And Security Issues In Fog

Vidyavathi D P[1], Sowmya C N[2], Sujata S Ratnakar[3]
[1, 2, 3] Lecturer, Dept of CS&E
[1, 2, 3] Government Polytechnic,Sriranga patna

Abstract- *Cloud computing is a general term for anything that involves delivering hosted services over the internet.A cloud can be private or public. A public cloud sells services to anyone on the internet. A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people, with certain access and permissions settings. Private or public, the goal of cloud computing is to provide easy, scalable access to computing resources and IT services. Cloud infrastructure involves the hardware and software components required for proper implementation of a cloud computing model. Though cloud has advantages, downtime is considered as one of the biggest potential downsides of using Cloud Computing. The cloud providers may sometimes face technical outages that can happen due to various reasons, such as loss of power, low Internet connectivity, data centers going out of service for maintenance, etc. In such cases "Fog computing" can be used.*

"Fog computing" which refers to extending cloud computing to an enterprise's network's edge. As a result, it's also known as Fogging or Edge Computing. It makes computation, storage, and networking services more accessible between end devices and computing data centers.Fog computing is the computing, storage, and communication architecture that employs EDGE devices to perform a significant portion of computation, storage, and communication locally before routing it over the Internet backbone.The goal of fog computing is to conduct as much processing as possible using computing units that are co-located with data-generating devices so that processed data rather than raw data is sent and bandwidth needs are decreased.

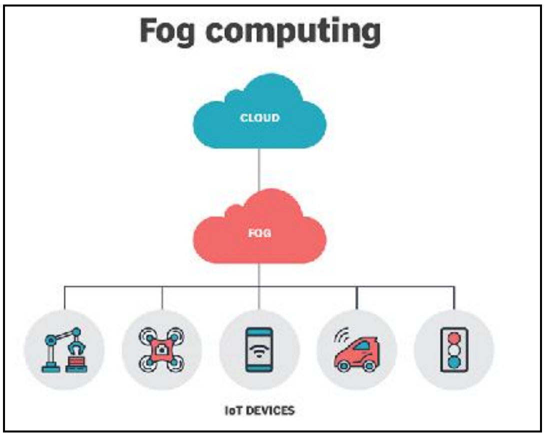
Keywords- Cloud computing,Fog computing, end devices, Layers

I. INTRODUCTION

Fog Computing is a model in which data is processed and applications which are concentrated in devices atthe network edge rather than existing almost entirely in the cloud. In general rather than sending the data directlyto the cloud from the smart devices it can be manage locally in the smart devices.Fog Computing creates that extension of cloud functionality when you need it and brings that functionality closer to where latency is very important.In the future 5G networks assure that latency will decrease aslow as possible like in sub-milliseconds so that the fastest network facility can be provided.For that the introduction 5G networks must support Fog computing.Fog computing is a platform which is virtually generated that gives the functionality to process, manage and other network services to the data between the cloud computing and a device

How does fog computing work?

Fog networking complements -- doesn't replace -- cloud computing; fogging enables short-term analytics at the edge, while the cloud performs resource-intensive, longer-term analytics. Although edge devices and sensors are where data is generated and collected, they sometimes don't have the compute and storage resources to perform advanced analytics and machine learning tasks.



Fog computing works by utilizing local devices termed fog nodes and edge devices. Raw data is captured by IoT beacons. This data is sent to a fog node close to the data source. This data is analyzed locally, filtered, and then sent to the cloud for long-term storage if necessary. Edge devices can be several different types of device, including:

- Routers
- Cameras
- Controllers
- Switches

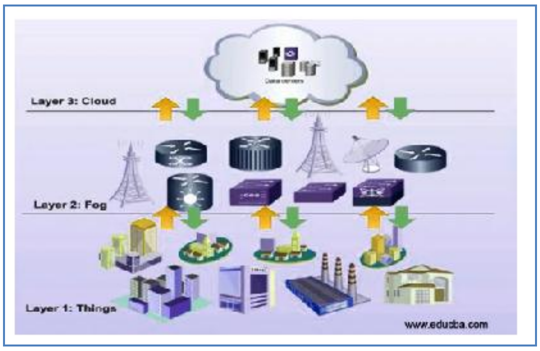
- Embedded servers

In reality, any device with computing, storage, and network connectivity can act as a fog node. When data is collected by IoT devices and edge computing resources, it is sent to the local node instead of the cloud. Utilizing fog nodes closer to the data source has the advantage of faster data processing when compared to sending requests back to data centers for analysis and action. In a large, distributed network, fog nodes would be placed in several key areas so that crucial information can be accessed and analyzed locally. far away to process the data and respond in a timely manner.

II. ARCHITECTURE

Hierarchical Fog Computing Architecture

The hierarchical fog architecture comprises of following three layers:



1. Terminal Layer

The terminal layer is the basic layer in fog architecture, this layer includes devices like mobile phones, sensors, smart vehicles, readers, smartcards, etc.

The devices which can sense and capture data are present in this layer. Devices are distributed across a number of locations separated far apart from each other.

The layer mostly deals with data sensing and capturing. Devices from different platforms and different architectures are mainly found in this layer..

2. Fog Layer

Fog layer includes devices like routers, gateways, access points, specific fog servers, and base stations etc., called as Fog nodes.

Fog nodes are located at the edge of a network. An edge can be a hop distance from the end device. The Fog nodes are situated in-between end devices and cloud data centers.

Fog nodes can be static, e.g., located in a bus terminal or coffee shop, or they can be moving, e.g., fitted inside in a moving vehicle.

Fog nodes ensure services to the end devices. Fog nodes can compute, transfer and store the data temporarily.

3. Cloud Layer

This layer consists of devices that can provide large storage and machines (servers) with high performance.

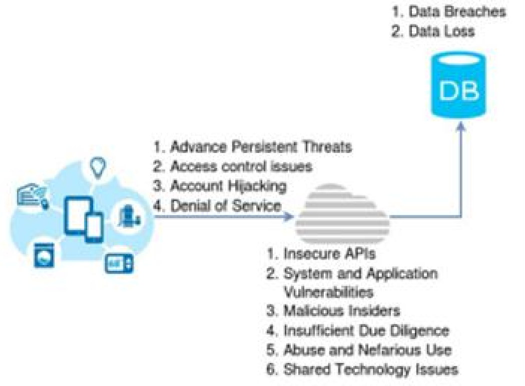
This layer performs computation analysis and stores data permanently, for back-up and permanent access to the users.

This layer has high storage and powerful computing capabilities.

Enormous data centers with high computing abilities form a cloud layer. The data centers provide all the basic characteristics of cloud computing to the users. The data centers are both scalable and provide compute resources on-demand basis.

III. SECURITY ISSUES

Fog computing have now been taken to increase the usability and potential of Cloud platform. With the advent of such wide applicability, the Fog and its similar platforms like Edge computing, Cloudlets and Micro-data centers are prone to attacks that can compromise Confidentiality, Integrity, and Availability. There are twelve critical security issues that directly impact distributed, shared and on-demand nature of cloud computing. Being a virtualized environment like Cloud, Fog platform can also be affected by the same threats.Our study considers following twelve security categories to formulate a systematic review:


1. Data Breaches
2. Data Loss
DB
1. Advance Persistent Threats
2. Access control issues
3. Account Hijacking
4. Denial of Service
1. Insecure APIs
2. System and Application Vulnerabilities
3. Malicious Insiders
4. Insufficient Due Diligence
5. Abuse and Nefarious Use
6. Shared Technology Issues

Potential security issues of Fog Platform inherited from Cloud computing. This figure shows how virtualisation and other issues of Cloud platform can effect Fog platform as well

1. Advance Persistent Threats (APT) are cyber-attacks whereby the aim is to compromise a company's infrastructure with the desire to steal data and intellectual property.
2. Access Control Issues (ACI) can result in poor management and any unauthorized user being able to acquire data and permissions to install software and change configurations.
3. Account Hijacking (AH) is where an attack aims to hijack the user accounts for malicious purpose. Phishing is a potential technique for account hijacking.
4. Denial of Service (DoS) is where legitimate users are prevented from using a system (data and applications) by overwhelming a system's finite resources.
5. Data Breaches (DB) are when sensitive, protected or confidential data is released or stolen by an attacker.
6. Data Loss (DL) is where data is accidentally (or maliciously) deleted from the system. This does not have to be resulting from a cyber-attack and can arise through natural disaster.
7. Insecure APIs (IA) Many Cloud/Fog providers expose Application Programming Interfaces (APIs) for customer use. The security of these APIs is pivotal to the security of any implemented applications.
8. System and Application Vulnerabilities (SAV) are exploitable bugs arising from software ad configuration errors that an attacker can use to infiltrate and compromise a system.
9. Malicious Insider (MI) is a user who has authorized access to the network and system, but has intentionally decided to act maliciously.
10. Insufficient Due Diligence (IDD) often arises when an organization rushed the adoption, design, and implementation of any system.
11. Abuse and Nefarious Use (ANU) often arises when resources are made available for free and malicious users utilize said resources to undertake malicious activity.
12. Shared Technology Issues (STI) occur due to sharing infrastructures, platforms or applications. For example, underlying hardware components may not have been designed to offer strong isolation properties.

IV. SECURITY AND PRIVACY IN FOG COMPUTING: CHALLENGES

1) Security

Fog computing security issues arise as there are many devices connected to fog nodes and at different gateways.
Though authentication plays a major role in establishing the initial set of relations between IoT devices and fog nodes in the network but this is not sufficient as devices can always malfunction or are also susceptible to malicious attacks.

2) **Privacy**

In fog computing, privacy preservation is more challenging since fog nodes may collect sensitive data. As a result, concerning the identity of end-users compared to the remote cloud server that lies in the core network.

Moreover, since fog nodes are scattered in large areas, centralized control is difficult.

3) Security and Privacy in Fog Computing: Challenges in IoT

Although IoT is in the boom, it delivers a variety of services to the end-users. It still faces many security and privacy issues.

Let us have a look at Security Privacy Internet of Things (IoT) issues.

4) Security issues

IoT devices are connected to desktops or laptops in our day-to-day life. Lack of security increases the risk of your personal information leaking while the data is collected and channeled to the IoT device.

IoT devices are connected to various networks. So, if the IoT device contains any security issues, it can be harmful to the end-users network. These issues can attack other systems and damage them.

5) Privacy issues

The main privacy issue is user information leakage in IoT devices such as data, location, etc.

As relations between IoT devices and fog nodes in the network play a major role which mitigates the impact of low latency, location awareness of many IoT applications.

V. CONCLUSION

Security and privacy are the major issues and are dealt efficiently in cloud computing but most of the existing technologies do not suit the fog computing due to the distinctive features of both along with along with vast range of fog devices. In addition to this new security and privacy concerns are to be faced for the first time as they were not present in cloud computing paradigm. This paper presents an overview of security and privacy issues in fog computing. The focal purpose of this study is to summarize the privacy and security issues in fog computing

REFERENCES

[1] Cloud-Fog Computing for Information-Centric Internet-of-Things Applications by Yung-Chiao Chen, Yao-Chung Chang, Chang-Hsu Chen , Yu-Shan Lin , Jiann-Liang Chen and Yu-Yao Chang

[2] Fog Computing Mitigate Limitations of Cloud Computing By Madhulika Bhatia, Shubham Sharma, Surbhi Bhatia, Mohammed Ali Alojail

[3] Fog computing with the integration of Internet of things: Architecture, Applications and Future Directions By HeenaWadhwaRajniAron

[4] Fog Computing and Security Issues: A review By Abdullah Aljumah , Tariq AhamedAhanger

[5] Fog Computing for Augmented Reality: Trends, Challenges and Opportunities By Shaik Mohammed Salman, Taufik Akbar Sitompul, Alessandro Vittorio Papadopoulos and Thomas Nolte

[6] Fog computing: Concept,Appliation and Future By XianghanZheng, Wei Wu, ChunmingRong, Tao Zhang

[7] Study of Fog Computing Structure-AbdukodirKhakimov , AmmarMuthanna, Mohammed Saleh Ali Muthanna

[8] MockFog: Emulating Fog Computing Infrastructure in the Cloud By Jonathan Hasenburg, Martin Grambow, Elias Grunewald, SaschaHuk, David Bermbach

[9] Fog Computing: A New Era of Cloud Computing By S. Delfin, Sivasanker.N.P, Nishant Raj

[10] Fog Computing- Network Based Cloud Computing By Y.Navaneeth Krishnan, Chandan N Bhagwat ,Aparajit P Utpat

[11] Fog computing security: a review of current applications and security solutions BySaad Khan, Simon Parkinson and Yongrui Qin