A Feasible Review on Cloud Computing Security Services with Recent technologies used in the Digital Channels

Jayachandran R[1], Dr. D. Malathi[2]

[1]Research Scholar, Department of CSE, SRM IST, Chennai, Tamil Nadu, India
[2]Professor, Department of CSE, SRM IST, Chennai, Tamil Nadu, India
[1]jr1116@srmist.edu.in, [2]malathid@srmist.edu.in

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: Fog computing plays a significant role in the field of cloud computing. Fog computing is termed as decentralization of data in the cyber world. This paper mainly focused on the feasible review of fog computing security with services and threats in the digital channels. This paper aims to explore the feasible study of fog computing with existing technologies, devices, and services from various research points of view. It's also described the systematic review and fundamental of fog computing. This paper summarized various digital channel techniques with fog computing and security threats in cyber networks based on the fog.

Keyword: Threats, Security, fog computing, decentralization, IoT, Big data

1. Introduction

Computing is the keyword used to determine the approximate values but not related to accuracy in general. Fog Computing is the process of data processed and stored in the cloud infrastructure between the origins. Fog computing is also termed as a centralized Cloud computing architecture process that minimizes the transmission of data overheads. It also improves cloud computing platforms' performance based on the requirements to process and store large volumes of enormous data. The fog computing mainly focused on the Internet of Things devices, based on the V3 concept (Sagiroglu S, 2013) such as volume, velocity, and variety of data generated from an array of devices.

IoT devices that provide high functionalities in-terms of connectivity of the network and improvement in innovation development with functionalities were motivated data. These devices mainly focused on various resources used for computing with appropriate data. These IoT devices mainly focused on fast processes in the decision and maintained a high level of functionalities. This high level of functionalities leads to scalability and issues in reliability by client-server architecture. The server processes every client details in the fog computing architecture. In the classical way of client-server architecture, when the client may increase, it leads to overload due to many devices facing issues during data processing. These issues can be overcome the fog computing, where the solution is decentralized, which introduces a new innovative hierarchically distributed. It's also accessible as an intermediate between the cloud computing system and the client as end-user devices, which shown in Fig.1

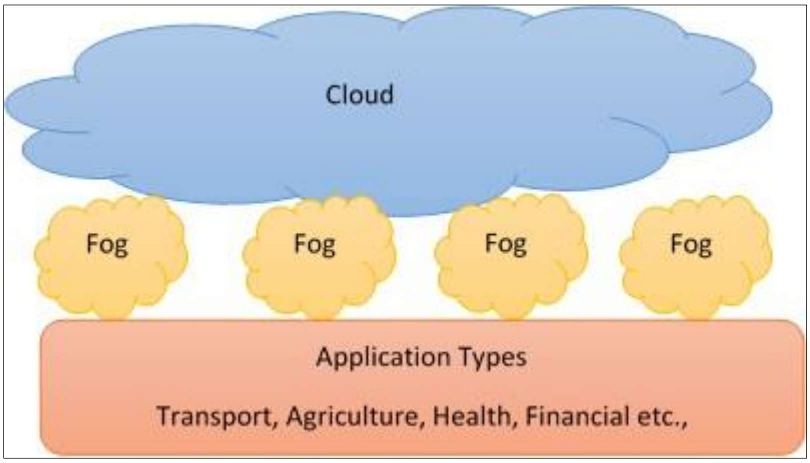
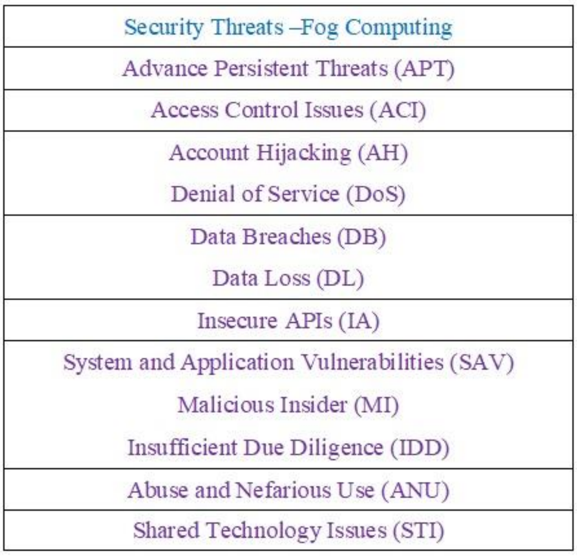


Fig.1 Fog Computing – Structure

From figure 1. Cloud computing which sub-categorized into various fog computing. Fog computing mainly focused on decentralizing data to avoid any issues when several devices connected with the server. The application can be of any domain to access the fog computing. This fog computing leads to increasing the processing speed, fast transmission of data, filtering process, which reduce the time and optimizing communication resources. These fog computing (Tang B, 2015)are analyzed by various authors, which can be observed in the following sections.

2. Systematic Review of Fog Computing

Cloud Security Alliance is the most significant concept in Fog computing, which subset of the cloud is computing. Twelve critical issues categorize Cloud Security Alliance in the security by the various researchers(Stojmenovic I, 2014)(Stojmenovic I W. S., 2015)(Yi S, 2015). The following figure.2 represent security threats in fog computing as below.



Security Threats –Fog Computing
Advance Persistent Threats (APT)
Access Control Issues (ACI)
Account Hijacking (AH) Denial of Service (DoS)
Data Breaches (DB) Data Loss (DL)
Insecure APIs (IA)
System and Application Vulnerabilities (SAV) Malicious Insider (MI) Insufficient Due Diligence (IDD)
Abuse and Nefarious Use (ANU)
Shared Technology Issues (STI)

Fig. 2. Security Threats- Fog Computing

From the figure, security threats with the following functionalities are observed by various researchers.

- Advance Persistent Threats(APT)→attack in the cyber network; data steal and property based on intellectual.
- Access Control Issues (ACI) →Management based on low quality and unauthorized user.
- Account Hijacking(AH) →Hijacking purpose
- Denial of Service(DoS) →User Protected from the system resources
- Data Breaches(DB)→Private and protected data
- Data Loss(DL)→ Accidentally or incidentally deleted from the system.
- Insecure APIs(IA)→Security of API's
- System and Application Vulnerabilities (SAV)→ Error based on software configuration.
- Malicious Insider(MI)→Authorized user doing the malicious process
- Insufficient Due Diligence(IDD)→ Meeting organization requirements
- Abuse and Nefarious Use(ANU)→ Resource to take malicious activities
- Shared Technology Issues (STI)→Hardware components have not been designed.

These are the technical issues faced in security issues in fog computing.

3. A Feasible Review of Fog Computing Services

Saad Khan et al. (2017) explained the significant role (Saad Khan, 2017)of fog computing resources used in the cyber world with decentralization architecture. It very well may be depicted as a cloud-like stage having comparable information, calculation, stockpiling, and application administrations; however, it is essentially unique in that it is decentralized. Fog frameworks can also prepare a lot of information locally, work on-premise, are completely convenient, and be introduced on heterogeneous equipment. These highlights make the Fog stage profoundly appropriate for time and area touchy applications. For instance, the Internet of Things (IoT) gadgets are needed to deal with a lot of information rapidly.

This wide scope of usefulness driven applications increases numerous security issues concerning information, virtualization, isolation, organization, malware, and checking. It reviews existing writing on Fog registering applications to recognize normal security holes.

Comparative innovations like Edge processing, Cloudlets, and Micro-server farms have additionally been incorporated to give an all-encompassing audit measure. Most Fog applications are inspired by the craving for usefulness and end-client necessities, while the security angles are regularly disregarded or considered an untimely idea.

This Researcher decides the effect of those security issues and potential arrangements, giving future security-significant bearings to those answerable for planning, creating, and keeping up Fog frameworks.

Deepika et al. (2017) described (Deepika 2017) fog computing various sorts of administrations, and every one of these administrations is gotten to through various AP (passages) or STB (set-top boxes). The haze processing foundation offers various types of assistance near customers or clients. Here and there, haze figuring acts like distributed computing.

Both figuring advances give application, stockpiling, information, and processing administrations to their enlisted customers. In any case, fog computing offers types of assistance near its end clients when contrasted with distributed computing that offers types of assistance distantly. Likewise, haze figuring gives thick topographical dispersion and having support for portability. This researcher gives a writing audit on Fog Computing Techniques.

Here and there, Fog Computing acts like distributed computing. Both processing advances give application, stockpiling, information, and figuring administrations to their enlisted customers. However, mist registering offers types of assistance near its end clients when contrasted with distributed computing that offers types of assistance distantly. Both Cloud and Fog give information, calculation, stockpiling, and application administrations to end-clients. In any case, Fog can be recognized from Cloud by its vicinity to end-clients, the thick geological appropriation, and its help for portability.

Jimoh Yakubu et al. (2019) proposed an innovative idea (Jimoh Yakubu, 2019)on Fog Computing is another worldview of figuring that stretches out distributed computing activities to the edges of the organization. The Fog Computing administrations give area affectability, diminished inactivity, topographical availability, remote network, and improved information streaming. Be that as it may, this processing worldview is anything but an option for distributed computing, and it accompanies various security and protection challenges.

This research work gives a deliberate writing survey on the security challenges in the fog computing framework. It surveys a few indispensable models to help the security of fog and afterward made a scientific categorization dependent on the different security methods utilized. These incorporate AI, cryptographic strategies, computational insight, and different methods that differentiate this research work, which provide the past surveys in this zone of exploration.

In any case, most of the proposed methods used to address security issues in haze processing proved unable to totally tend to the security challenges because of the different strategies' restrictions. This survey is expected to direct specialists and fledgling analysts to recognize certain regions of security challenges in haze registering for future upgrades.

Malka N Halgamugem et al. (2018) proposed the Internet of Things, gadgets, and distant server farms need to interface. The motivation behind(Malka N. Halgamugem's 2018) mist is to lessen the sum of information shipped for handling, examination, and capacity to accelerate the registering measures. The hole between fog computing innovations and gadgets needs to limit as development in business today depends on the ability to interface to advanced channels to prepare a lot of information. Distributed computing is impossible for some internet of things applications; in this manner, mist registering is frequently seen as a practical option for IoT benefits. It has empowered a broad assortment of advantages, suchas diminished data transmission, decreased dormancy, and upgraded security.

Nonetheless, IoT Devices set at the edge of the web have met various protection and security dangers. Anyway, fog computing devices that are put at the edge of the web have met various protection also, security dangers. This exploration work plans to look at and feature security and protection. It gave mist registering through an exhaustive audit of late distributed writing of mist registering and recommend arranging recognized issues.

4. Comparison of Fog Computing based on Digital Channels

The comparison of fog computing based on the above four researchers are summarized in the following table.1 as follows

Authors	Services	Devices	Technologies

Saad Khan et al. (2017)	a) Support for Mobility
	b) Thick Geographical Distribution
	c) QoS
		AP(Access Point)
		STB(Setup Boxes)
			Big Data

Deepika et al. (2017)	a) Identify common security gaps. b) Heterogeneous Hardware c) Time and Location Sensitive application	Cisco Fog Computing	IoT
Jimoh Yakubu et al. (2019)	a) Taxonomy Based Security Techniques b) Cryptographic Techniques c) Computational Intelligence	Large Scale Senor Network	IoT and Big Data
Malka N Halgamugem et al. (2018)	a) Decrease Bandwidth b) Enhance Security c) Reduce Latency	Digital Channel for a Large amount of data	Big Data and IoT

Table 1: Comparison of Fog Security

5. Summarization of Security

The List of security attacks involved in the possible attacks of fog computing.

Attack Category	Possible Threats
Virtualization Issues	• Hypervisor Attacks • VM-Based Attacks • Service Abuse
Web Security Issues	• SQL Injection • Drive-by attacks • Cross-site scripting
Internal /External Communication issues	• Middle attack • Poor access control • Single point of failure
Data Security Related Issues	• Data Replication • Data Altering • Multi-tenancy issues
Wireless Security issues	• Active impersonation • Message reply attacks • Data Loss
Malware Protection	• Virus • Trojans • Spyware

6. Conclusions

A Feasible review of fog computing with the fundamental concept and systematic review in the cyber network is concluded. This paper explored fog computing's technical concepts with appropriate threats described by the various researchers involved in the research work related to fog computing. This paper summarized the various devices, techniques, and services involved in fog computing by various researchers in the wireless sensor network. The paper provides effective and efficient information on fog computing services with recent technologies in the cyber world.

Reference

A. Barenji, A. V. (2021). Toward blockchain and fog computing collaborative design and manufacturing platform: Support customer view. *Robotics and Computer-Integrated Manufacturing*.

B. Deepika, K. R. (2017). A Literature Review on Fog Computing. *International Journal of IT and Knowledge Management*.

C. Jimoh Yakubu, H. A. (2019). Security challenges in the fog-computing environment: a systematic appraisal of current developments. *Journal of Reliable Intelligent Environments*, 209-233.

D. Karimiafshar, A. M. (2021). A request dispatching method for efficient use of renewable energy in fog computing environments. *Future Generation Computer Systems*, 631-646.

E. Li, K. (2021). Heuristic Computation Offloading Algorithms for Mobile Users in Fog Computing. *ACM Transactions on Embedded Computing Systems (TECS)*, 1-28.

F. Malka N. Halgamugem, E. B. (2018). Security and privacy issues of fog Computing for the internet of things (IoT). *n Cognitive Computing for Big Data Systems Over IoT*, 139-174.

G. Saad Khan, S. P. (2017). Fog computing security: a review of current applications and security solutions. *Journal of Cloud Computing*.

H. Sagiroglu S, S. D. (2013). Big data: A review. In: Collaboration Technologies and Systems. *International Conference On IEEE.*, 42–47.

I. Stojmenovic I, W. S. (2014). The fog computing paradigm: Scenarios and security issues. *In: Computer Science and Information Systems*, 1-8.

J. Stojmenovic I, W. S. (2015). An overview of fog computing and its security issues. *Concurrency and Computation: Practice and Experience*.

K. Tang B, C. Z. (2015). A hierarchical distributed fog computing architecture for big data analysis in smart cities. *In: Proceedings of the ASE BigData & SocialInformatics*.

L. Yi S, Q. Z. (2015). Security and privacy issues of fog computing: A Survey. *In: International Conference on Wireless Algorithms, Systems, Springer.*, 685–695.