International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May-2018 www.irjet.net p-ISSN: 2395-0072

Survey on Fog computing and its application benefits in real life

K.Saranya[1], Jaya prakash.J[2], Sethu Balaji.K.G[3]

[1] *Assistant Professor, Department of Computer Science and Engineeering, Kumaraguru College of Technology, Coimbatore, Tamilnadu,*
[2,3] *Student, Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore, Tamilnadu.*

ABSTRACT- *Fog computing is also said to be fogging /edge computing, fog is a model developed for data processing, application services and concentrated on user devices at the network edge rather than in existing type called cloud computing. In this article, the basic idea of fog computing is discussed and ,how does fog computing work along with a brief comparison table between Fog nodes closest to IOT devices, Fog aggregation nodes and Cloud, and a detailed literature survey was carried out on fog computing's security and discussed about existing system called cloud computing ,proposed system called fog computing and conclusion*.

I. INTRODUCTION

Cloud computing is an environment created in a user's machine from an on-line application stored on the cloud and run through a web browser. In simple Cloud computing is using the internet to access someone else's software running on someone else's hardware in someone else's data center. But since cloud computing has several disadvantages like it has high latency, security, high data movements, high bandwidth, cost, infelexbility, high speed internet connection required. To overcome some disadvantage of cloud computing, fog computing was introduced by cisco systems. Fog computing it is also said to be fogging /edge computing, it is a model, developed for data processing, application services are concentrated on user devices at the network edge rather than in existing type called cloud computing The remaining of the paper is structured as follows. section ii is the literature. section iii is about the existing system .section iv is about the proposed system. section v is about conclusion.

II. LITERATURE SURVEY

Pengfei Hu, said about Face identification and resolution technology is so crucial to ensure the identity of humans in physical space and cyberspace. There are increase in application based on face identification and resolution in Internet of Things (IoT) and big data which raises the demands of computation, communication, and storage capabilities. Therefore, to improve process capacity and bandwidth the fog computing-based face identification and resolution framework has been proposed. Even though there are problems arising in security and private issues due to properties of fog computing-based framework. This paper we discuss about security and privacy reservation scheme as a solution to the above issues. There will be outline of the fog computing-based face identification and resolution framework and also the summarization of security and privacy issues. To solve the issues of confidentiality, integrity, and availability in the processes of face identification and face resolution, systems were proposed like the authentication and session key agreement scheme, data encryption scheme, and data integrity checking scheme were proposed. At last the prototype system is introduced to evaluate the influence of security scheme on system performance. Not only that we also evaluate and analyze the security properties of proposed system scheme from the viewpoint of logical formal proof and the confidentiality, integrity, and availability (CIA) properties of information security. The results what we obtained is the introduced proposed scheme can meet the requirements for security and privacy preservation effectively.

[2]. Abdulrahman Alhothaily, ChunqiangHu,and Arwa Alrawais has discussed that Fog computing is like a bridge which has been introduced to bridge(i.e TO FILL) the gap between remote data centers and Internet of Things (IoT) devices. Fog is an appropriate paradigm for many IoT services by enabling a wide range of benefits which also includes enhanced security, decreased bandwidth, and reduced latency . However the fog devices (located at the edge of the Internet) obviously face many security and privacy threats. In this paper the author discuss about the security and privacy issues in IoT environments and they propose a mechanism for security enhancement among IOT devices which employs fog computing to improve the distribution of certificate revocation information among them.

[3]. Javier Lopeza , Masahiro Mambob, Rodrigo Romana , have discussed about the various reasons why the cloud computing paradigm is unable to meet certain requirements (e.g. low latency context awareness, mobility support) that are crucial for several applications (e.g. vehicular networks, augmented reality). The various paradigms, such as fog computing, mobile edge computing, and mobile cloud computing, have emerged in recent years to fulfill the above requirements in which fog computing contributes a lot serving as a edge node between IOT and cloud. Also the edge paradigms share several features, most of the existing research is compartmentalised; no synergies have been explored which is especially true in the

field of security, where most analyses focus only on one edge paradigm, while ignoring the others. The main goal of this paper is to holistically and completely analyse the security threats, challenges, and mechanisms inherent in all edge paradigms, while highlighting potential synergies and venues of collaboration. The paper says the authors will show that all edge paradigms should consider the advances in other paradigms.

[4]. K Gurnadha Gupta , Geetha Kurikala1 ,A.Swapna ,Assistant Professor have discussed that. The data in cloud network is less secure (i.e The data is vulnerable) and to defend the data on cloud from attacks by hackers, mainly corporate industries executive attacks to defeat their competitors . In cloud server oversized and private information are kept. Many business people are using cloud network storage to store data of huge amount. As many and many are using cloud storage the vulnerability of data which is stored in cloud will be increasing. the data in cloud are accessed by computer systems by communication and network which leads to new information security challenges. preventing information felony attacks is unsuccessful on cloud with subsisting ways of protective secure and vital information. For securing the data a new approach is introduced in addition to cryptography mechanisms. A novel profile is created ,monitored and updated to server for every user individually. The misinformation attack is launched when there is unauthorized permission or untargeted hunt for information detected. The owner of information or user who ever try to access the data they need to answer the questions first. The decoy(i.e duplicate) information is provided for some illegal user to protect the owner's real data.

[5]. Tom H. Luan ,Guiyi We , Zhi Li , Yang Xiang , Longxiang Gao and Limin Sun have discussed about smart devices, particular smartphones, becoming our everyday companions, the mobile Internet and computing applications pervade people's daily lives. Huge demand for high-quality mobile services at anywhere and anytime is the cause, which leads to a question (how to address the ubiquitous user demand) next generation mobile networks. The optimal solution for the above mentioned problem is Fog computing paradigm Fog computing introduced to reduce many difficulties in which extending cloud computing by providing virtualized resources , engaged location-based services to the edge of the mobile networks is also one, which is to reduce serve mobile traffics. application module, service module, management module, security modules and storage module, then the front end and backend are connected through internet connectivity. The combination of lubricant of cloud computing and mobile applications is fog computing. The paper describes the outline of fog computing like design, architecture and network research knowledge.

[6] Saad Khan, Yongrui Qin,Simon Parkinson have discussed about fog computing. Fog computing is a new paradigm which provides computing resources on the edges of a network by extending the Cloud platform model. The fog computing is different from cloud platform even though it is having similar data, computation, storage and application services . Fog systems has advantages like operate on-premise, fully portable, processing large amounts of data locally, and it can be installed on heterogeneous hardware. The Fog platform is highly suitable for location-sensitive and time-sensitive applications with the help of above mentioned advantages . If we take an real time example, Internet of Things devices must quickly process a large amount of data in less time. Security issues regarding data, network, virtualization, segregation, malware and monitoring are wide range of functionalities of fog computing. Literature on how the gap is filled by fog computing is explained here and also technologies like Edge computing, Cloudlets and Micro-data centres are also included .The end-user requirements and functionality motivates the major fog applications, regardless to some security issues. The result what we will obtain is to know the causes of security problem and their solutions. Design, development and maintaining fog systems are also it's responsibilities.

[7]NANZHANG, YANSUN, FUHONGLIN have discussed about fog computing. It is defined as distributed computing paradigm at the edge of the network and it requires cooperation of users and sharing of resources. When fog computing users open their resources (i.e. their devices) which are easily intercepted and attacked, as they are accessed through wireless network and there is a extensive geographical distribution. To supervise user's behavior and the security of user they have introduced credible third party in this study. Based on the human nervous system fog computing security mechanism is proposed and the strategy for a stable system evolution is calculated . Using the proposed system it is observed that the number of attack behaviors have reduced effectively in accordance with MATLAB simulation results.

[8] Kuan Zhang,Jianbing Ni, Xiaodong Lin have discussed about fog in IOT. Internet of Things (IoT) is used to connect billions of device for application such as home automation ,smart cities , and environmental monitoring by the process of collecting and exchanging data between connected devices. Even though IOT has above mentioned features ,it also has unsupported features (e.g., low latency, location awareness, and geographic distribution) which are critical for some IoT applications such as smart traffic lights, home energy management and augmented reality. Fog computing is introduced to support these features. Using fog computing in IOT leads to extend computing, storage and networking resources to the network. On the other hand it is inferred that there might be various security and privacy issues for users. Fog computing architecture and it's features are reviewed .And also real-time services, transient storage, data dissemination and decentralized computation which are critical roles of fog node have been studied . Every fog associated IOT applications like home automation etc.., are tested using different roles of fog.

After that security and privacy threats to IOT are mentioned. The solution to security and privacy threat in fog computing IOT application is obtained by new architecture.

Following table describes the various security features discussed in several papers,

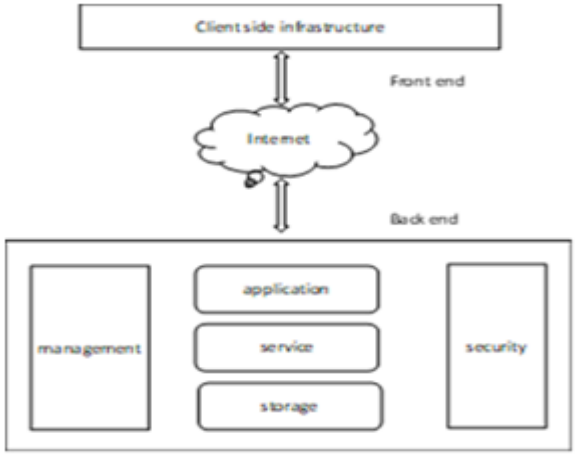
s. no	Paper	Technology used	Pros and cons
1.	Security and Privacy Preservation Scheme of Face Identification and Resolution Framework Using Fog Computing in Internet of Things.	Face identification	[P] it is fully automated. [C]It fails in low lightning condition.
2.	Internet of Things: Security and Privacy Issues	Enhancing security using iot	[P] costsaving and instand data access. [C]It is complex and has less privacy.
3.	A Survey and Analysis of Security Threats and Challenges	Virtual machine	[P] Disaster recovery is quick. [C]server side problem may occur
4.	Implementation of Security and Privacy to Comprehensive Approach for Avoiding Knowledge Thieving Attack Exploitation Decoy Technology	Decoy technology	[P] detection of masquerade
5.	Focusing on Mobile Users at the Edge	Network function visualization	[P] Improved operational simplicity. [C]It require more dynamic than traditional ones.
6.	A review of current applications and security solutions	Data encryption	[P] Encryption Equals Confidentiality. [C]Unrealistic Requirements.
7.	A security mechanism based on evolutionary game in fog computing	MatLab simulation	[P] programming is simple. [C]when more GUI are build then performance will be low
8.	Securing Fog Computing for Internet of Things Applications: Challenges and Solutions	IOT	[P] costsaving and instand data access. [C]It is complex and has less privacy.

III.EXISTING SYSTEM

Cloud computing is An environment created in a user's machine from an on-line application stored on the cloud and run through a web browser. In simple Cloud computing is using the internet to access someone else's software running on someone else's hardware in someone else's data center. There are three major services are provided by cloud,

- Software as a Service (SaaS) – It is used by End Users.
- Platform as a Service (PaaS)- It is used by Application Developers.
- Infrastructure as a Service (IaaS)-it is used by Network Architects.

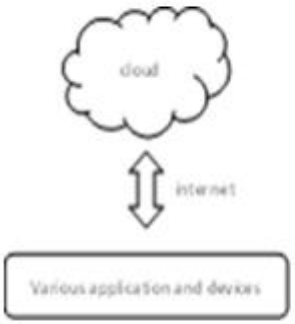
There are three types cloud used as per the requirement, 1.public cloud, 2.private cloud, 3.hybrid cloud. Then, public cloud is Computing infrastructure hosted by cloud vendor at the vendors premises and can be shared by various organizations, private cloud is a computing infrastructure dedicated to a particular organization and not shared with other organizations. more expensive and more secure when compare to public. hybrid cloud are Organizations may host critical applications on private clouds where as relatively less security concerns on public cloud. usage of both public and private together is called hybrid cloud. By using this we can reduce amount of e-waste. Some of Cloud operating system used are, Eye os, Ameoba os, glide os, my goyo etc…,



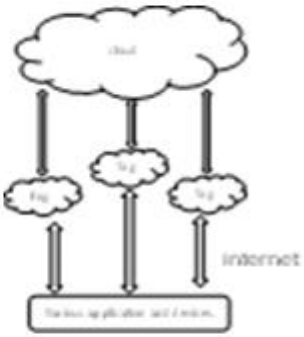
Figure[1]

Figure[1] show the architecture of cloud computer where front end has client side infrastructure ,back end has several modules like application module, service module, management module, security modules and storage module, then the frontend and backend are connected through internet connectivity.

IV.PROPOSED SYSTEM



Figure[2]



Figure[3]

Fog computing is also said to be fogging /edge computing, fog is a model developed for data processing, application services and concentrated on user devices at the network edge rather than in existing type called cloud computing. unlike cloud computing ,fog computing devices are distributed on spanning multiple domains, heterogenous platforms.to overcome disadvantage of cloud computing ,fog computing was developed by cisco systems. Fog computing is more secure than cloud computing. Fog extends cloud computing extends cloud by placing intermediate node as shown in below figures, Figure[2] shows how application and devices are connected to cloud and Figure[3] shows how the application and devices are connected to intermediate fog and then to cloud. Using of fog computing reduces the data movement when compared to cloud, and fog has greater security level than cloud. fog allows faster upload and download of data.

V. CONCLUSION

Fog computing is developed for emerging network that requires faster processing with minimum level of delays. It is also designed to manage large amount of data.by using fog computing we can provide much user experience. It provide services many domains like IoT wireless network with sensors, smart grid and SDN(software defined network).we have examine several security types comparative study.

REFERENCES:

Website:

https://www.cisco.com/

Paper:

1. Pengfei Hu, Student Member, IEEE, Huansheng Ning, Senior Member, IEEE, Tie Qiu, Senior Member, IEEE, Houbing Song, Senior Member, IEEE, Yanna Wang, and Xuanxia Yao

2. Arwa Alrawais, Abdulrahman Alhothaily, Chunqiang Hu, and Xiuzhen Cheng George Washington University

3. Rodrigo Romana , Javier Lopeza , Masahiro Mambob aComputer Science Department, University of Malaga, Ada Byron building, 29071 Malaga, Spain. bFaculty of Electrical and Computer Engineering, Institute of Science and Engineering, Kanazawa University, Kakuma Kanazawa 920-1192, Japan.

4. Geetha Kurikala1 , K Gurnadha Gupta ,A.Swapna ,Assistant Professor, Department of Computer Science and Engineering, Sri Indu College of Engineering & Technology, Telangana, India

5. Tom H. Luan , Longxiang Gao , Zhi Li , Yang Xiang , Guiyi We , and Limin Sun ,School of Information Technology, Deakin University, Melbourne Burwood, VIC 3125, Australia , School of Computer Science and Information Engineering, Zhejiang Gongshang University, Zhejiang, China .,Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

6. Simon Parkinson ,Yongrui Qin.Saad Khan,

7. YanSun,FuhongLin, NanZhang, King Saud University

8. Jianbing Ni,Kuan Zhang,Xiaodong Lin ,Canada