Proceedings of the SMART–2016, IEEE Conference ID: 39669
5th International Conference on System Modeling & Advancement in Research Trends, 25th–27th November, 2016
College of Computing Sciences & Information Technology, Teerthanker Mahaveer University, Moradabad, India

Fog Computing: Common Security Issues and Proposed Countermeasures

Praveen Kumar[1], Nabeel Zaidi[2] and Tanupriya Choudhury[3]
[1,2,3]Amity University, Uttar Pradesh, India
E-mail: [1]pkumar3@amity.edu, [2]khizerzaidi@gmail.com, [3]tchoudhury@amity.edu

***Abstract*—Fog computing is one of the most important paradigms used in modern world as an extension to cloud computing. Like Cloud Computing, it provides data storage, manipulation and computation of data, but to the edge of the network, i.e. to the user end. This research paper deals with the threat to security issues, especially with location privacy and data confidentiality. The way service providers as well as government can access users data is covered. Furthermore the misconceptions about the rights of users are discussed. Finally the concept of decoy technique with some modification for location and data privacy is also covered.**

Keywords: Fog Computing, Cloud Computing, Security, Privacy, Decoy Technique

I. Introduction

The popularity of smart devices connected everywhere are shaping the future of the modern world. The way technologies are being developed such as smart metering system,[2] smart wearable devices, smart cities as well as large scale sensor development are making everything smarter and connected, described as Internet of things (IoT). According to new research from International Data Corporation (IDC), "The worldwide Internet of Things (IoT) market will grow from $655.8 billion in 2014 to $1.7 trillion in 2020 with a compound annual growth rate (CAGR) of 16.9%.Devices, connectivity, and IT services [1] will make up the majority of the IoT market in 2020." Usually we know, there are many problems faced by smart devices such as battery issue, storage, slow response time as well as computation power which ultimately lowers the quality of the device and overall experience by the user. In order to overcome such problems faced by the smart devices, fog computing is acknowledged as an assuring computing standard, which can deliver data to the edge of the network/ to the user end in a way such that there is better[5] quality reassured of infrastructure, platform and software as well as at low relative cost.

Cloud and fog computing are the two software paradigm that cannot completely overtake one another as both are equally important. Hence, Fog computing is a not complete solution. Even there are many problems which are unsolved as Internet of things (IoT) applications require most important information about the user such as geo-distribution, mobility support, location awareness as well as low latency. More Importantly Fog (Edge) Computing is proposed to enable computing directly at the edge of network so that data can be transferred instantly to billions of services and applications that are connected. A way to look at the layers of fog computing is to consider it as a virtual platform that is located between the cloud centers and the devices as shown in Fig. 1. Typical example of fog computing devices is Wireless Sensors and Actuators Networks (WSANs), Google glass, cellular base stations etc. Fog Computing supports a variety of different services and application such as big data analysis, web content delivery, and augmented reality.[10]

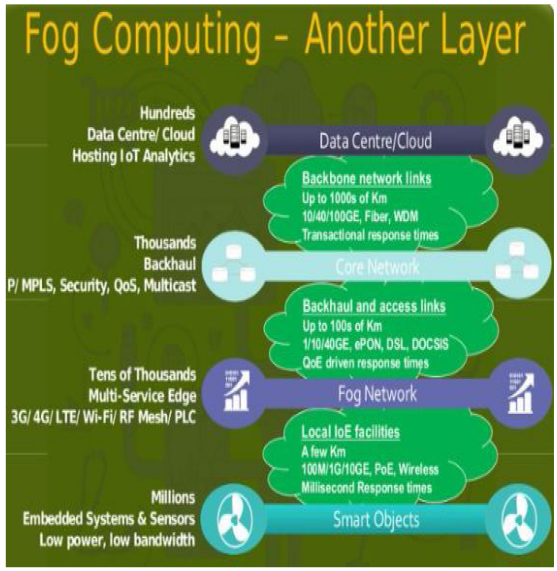

Fig. 1: Layers of Fog Computing [4]

Though fog is an important extension of cloud computing, so there are some security and privacy concerns which are unavoidable and have a great impact on it. Since these [3] issues if not properly taken care of will only impact the promotion of fog computing. We can see the comparison of IaaS adoption in public, hybrid and private cloud in Fig. 2. As Fog is in its developing phase, and is proposed in context to Internet of things, security

issues are inherited by it from the cloud. While some problems are inherited while there are new problems that occurs due to distinct feature of fog computing such as location awareness, low latency, mobility support required, large no. of geo-distributed nodes and different types of fog node and network.[11]

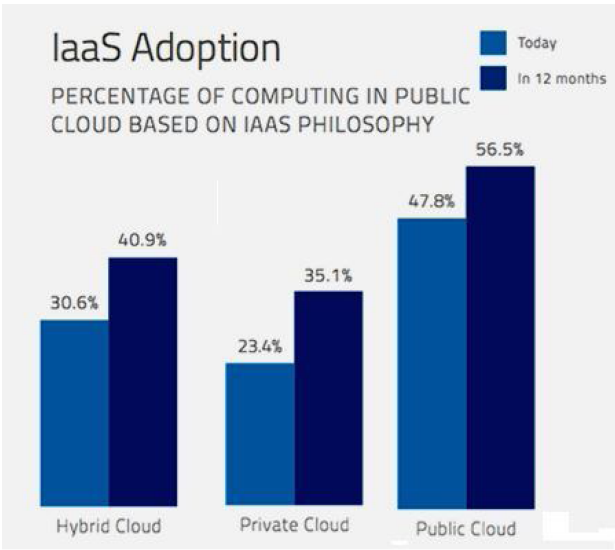

Fig. 2: Barriers to Fog Computing [2]

II. Fog Computing Overview

Here, we will give an overview of fog computing. It is assumed that readers are familiar with the cloud and mobile cloud computing and if possible can refer to different sites on internet. Fog computing extends the cloud computing so it can be closer to the things that produce and act on Internet of things (IoT) data. These things which are at user-end are called fog nodes and can be used anywhere within a network connection. Fog nodes are those devices with the ability to compute, store and can be connected to a network connection. For Examples- switches, routers and video surveillance camera etc.

Keeping the vision in mind, a brief definition was proposed during 2014 as a case in which a very large number of heterogeneous (sometimes autonomous and wireless) ubiquitous as well as decentralised devices communicate with each other and devices capable of cooperating with each other and processing data without the involvement of third parties. Most of these tasks are for supporting the functions of basic network or services which are new as well as those applications which run in a sandboxed environment[12]. Users leasing part of their devices [1] to host these services get incentives for doing so. In fact these definition are contradictive in nature but the term fog computing is not at all a fuzz word. Fog computing has its own advantage but there are many disadvantage which we will be focussing in our paper.

III. Security and Privacy Issues of Fog Computing

A. Network Security

Development of wireless technology has led to the bigger issues in security. Fog computing is effected in a similar ways like other wireless technology is affected. Various examples of such attacks are sniffer, spoofing, jamming etc. These attacks normally take place between the fog node and the centralized system. Generally, we are bound to trust the configurations generated by our network administrator, which separates [8] the normal data traffic from our network. Hence it brings a lot of burden to the network manager. Furthermore fog nodes are at the edge of the network, which only increases the burden of the network manager. SDN (Software Defined Networking) can be used as an approach for the network manager to work at the low level of abstraction for the network services. It can help in management, increase scalability of network as well as reduce cost with reference to fog computing. We can use Network Monitoring and Intrusion Detection System [2] to watch the traffic, Traffic Isolation and Prioritization system can be used to prevent attack by shared resources, Network resource access control system helps to get access control on SDN (Open Control), Network Sharing System can help the fog node router to be open to guests considering the security issues as well.

B. Data Security

In fog Computing User's control to data is overtaken by fog node, hence the same security issues arise of cloud computing. Data Integrity cannot be hold as data may be lost or can also be modified. The data which is uploaded to the fog node can also be used by the third party. There are various techniques that can [5] be used to provide data Integrity, confidentiality and verifiability such as combination of homomorphic encryption and searchable encryption. These techniques make sure that client does not store data on untrusted server. Cao et al has made schemes using the LT code which considers the storage(less) a primitive factor, also the data can be retrieve in a much faster way and hence the communication cost becomes low. There are always new challenges in fog computing related to the designing of the [9] storage system which can deal with the dynamic operations in a much faster way and takes less space.

C. Access Control

Access control is one the most important tool to assure the system's security and sustain the user's privacy. Although usually access control is labelled to the same domain but due to the distributive nature of cloud computing, it is implemented cryptographically. There are many proposed solution to achieve exquisite solution. One of them is of Yu et al in which the access control is based

 ISBN: 978-1-5090-3543-4

on Attribute-based encryption (ABE). There are even theories in which policy based access control mechanism is applied to handle the heterogeneous nature of fog computing. It is always a challenging task to keep in mind resource constraints and yet design the access control structure for the fog.

D. Privacy

The way privacy of a user is not sustained had made this issue of serious concern. Not only the service provider but the fact that Government too is involved in it makes it more challenging. In fact it even become easier for the third party to gain access to the user's private data, location etc. And hence the user becomes attack-prone. Due to data delivery at the edge of fog node, it becomes lot easier to collect all the important information of a user. This is one of the most challenging issue in fog to preserve the privacy of a user.

1) Privacy of data and usage

There are many data's privacy preserving algorithm available in the market but most of them uses the concept of resource prohibition at the edge devices. We know usually fog node collects all the important data generated for its efficient use and because of it homomorphic encryption [3] concept can be utilized. Even when the fog nodes collects information it has all the vital information such as when the user is at home, who else is with him etc.we must make sure that this data must not be delivered to the third party. One possible solution is to generate more dummy traffic and load them to the fog nodes, so that no one can identify the original data.

2) Privacy of location

Privacy of location usually refers to location privacy of the user at the edge of fog computing. As the data is delivered to the end of the fog node, it may be used to find how far the user from other fog nodes is. Moreover, if the client is using many fog services, one can easily know the path data has taken and hence our privacy location is at risk. Usually fog client chooses the nearest fog server, and thus can easily be vulnerable to attacks as the fog nodes know the location of the client. One such technique of preventing the violation of location privacy in fog computing is "identity obstruction". In it the fog node cannot easily identify exactly the nearest fog client among many others. There are lots of methods available to use identity obstruction technique for example, we use a third party fake id generator at each end user so that fog client has many options available to choose fog node from. Basically, fog client[2] does not use the nearest fog node at his/ her own will but actually the fog node is selected based on some criteria such as load balance, reputation, latency etc. Hence the fog node has only rough idea about location of fog client but not exact location. Furthermore even after using obstruction technique fog client is not secure as its location still can be jotted down by intersecting multiple fog nodes in an area since fog client uses multiple fog nodes of an area.

The concept of fog computing at user end can provide rich information about the network, its traffic information, its client information which can be used for optimization. The location information may become dangerous for both side – client end as well as fog nodes. One can easily get the location of client end if it's a fog node and of fog node if it's a client end. Although it's very important for efficient running of devices. Similarly both fog and cloud plays an important role in location privacy as fog can give an overview locally while cloud gives globally.

E. Attackers Interest in Private Data

Generally attackers can be broadly divided into three groups-Cloud Service Providers, Hackers and Governments. They usually have interest in user's private data in cloud.

1) Cloud service providers

Cloud service providers wants to gain users private data for further improvement most of the time. But unlike hackers, they legally authorised to access these data because they already had made user to accept their terms and agreements. Even without the knowledge of a user they use these data for advertisements and also for predicting what things a user can buy or what thing is popular in that area.

a) Terms and Conditions of Cloud Service Providers: It is very important for the user to read the terms and conditions before accepting them. Most of the times it written[6] that the service provider is not responsible for any misuse of the data and also does not guarantee data confidentiality. They also can modify, delete the data without any prior notice to the user. Not only that they can disclose information to the third party users. Moreover, it is important to note that Terms of Service (TOS) can change without any prior notice. Thus it is important to note that some service providers are making use of user's lack of knowledge about privacy issues.

Here are some of the evaluation of Terms Of Service (TOS) of few and famous service providers:

i) Google Cloud PlatformTerms of Service: Following are some of the sentences from Terms of services of Google cloud:

1. If Google makes a material change to the Services, Google will inform Customer, provided that Customer has subscribed with Google to be informed about such change. Basically they will only let those users know about the modifications who are subscribing them what about the others?
2. Google reserves the right to review the Application, Project, and Customer Data for

compliance with the AUP. Hence our whole project will be reviewed from time to time even if we don't want to.

3. If a Data Location Selection is not covered by the Service Specific Terms (or a Data Location Selection is not made by Customer [5] with respect to any Customer Data), Google may process and store the Customer Data anywhere Google or its agents maintain facilities. Google needs to inform them where there data is stored if there prescribed data store location is not present.
4. "Google reserves the right to terminate the Terms with you or discontinue the APIs or any portion or feature or your access thereto for any reason and at any time without liability or other obligation to you." Therefore Google has every right to terminate a user from using its service at any time whenever it went by providing any reason they want.

ii) Yahoo Cloud Terms of service: Yahoo which is sold to Verizon in year 2016 has similar terms of services as that of Googlecloud [9] but also has more loop holes for violating user's privacy. Following are some of the terms of services of yahoo cloud.

1. You also understand and agree that the Yahoo Services may include certain communications from Yahoo, such as service announcements, administrative messages and the Yahoo Newsletter, and that these communications [1] are considered part of Yahoo membership and you will not be able to opt out of receiving them. Thus we are bound to receive these messages, mail etc. everytime even when we are busy.
2. You are responsible for obtaining access to the Yahoo Services, and that access may involve third-party fees. Accessing yahoo services may sometimes involve third party hidden fees which in most cases we are unaware of.
3. You acknowledge, consent and agree that Yahoo may access, preserve and disclose your account information and Content if required to do so. Hence user's privacy is at greater risk.

The Figure below shows the bar graph created by going through the various responses at the policechiefmagzine.org which is the enforcement agency by professionals throughout the United States and also from various other data[7] such as information week surveys. We can see that there is about 2.5 i.e. 50 percent risk from Cloud service Providers.

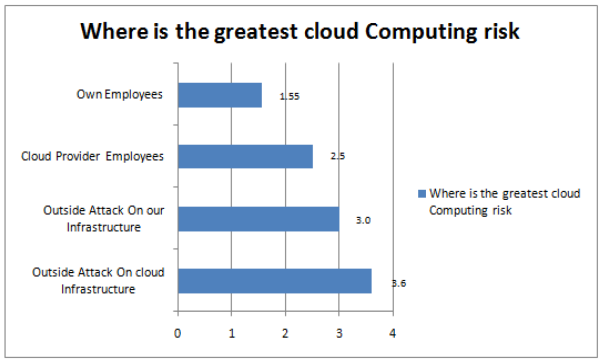

Fig. 3: Cloud/Fog Risk

2) Government: Government can easily access user's private data legally. They can force the Service Providers to give them information which was otherwise encrypted and protected. This disclosure of information may be due to terrorism or surveillance etc.

3) Hackers: Hackers uses user's private data for illegal activities such as to promote terrorism. Credit card information,[9] bank details, health records are some of the data which is of great interest to hackers. They may get millions by selling these data to third party organization.

IV. Proposed Approach for Privacy Protection

We Combine various techniques and propose theoretically a new technique for data and location Privacy. Firstly for location privacy we use a similar decoy technique with additional benefits. We make fake nodes at every fog connection as well as fake documents and deliver the attacker towards the path of fake fog node making it looks like legimate and original. We then make the unauthorised user to download the fake documents. Furthermore these fake documents will contain the hidden batch file which will run automatically in the background, the moment that user runs it. This batch file can be used to send the information about the user such as mac address, ip address etc to the regional cloud so that it can further block request. Although we can easily find ip address from the regional cloud for the devices that are connected but taking in view that the ip address may be fake, so our theoretically technique will work on the basis of mac address which though can be hidden but can never be changed. Hence we use that unauthorised user's system to find out his mac address and deliver it to the regional cloud so that his further request will be blocked and also we will have a rough idea of his location.

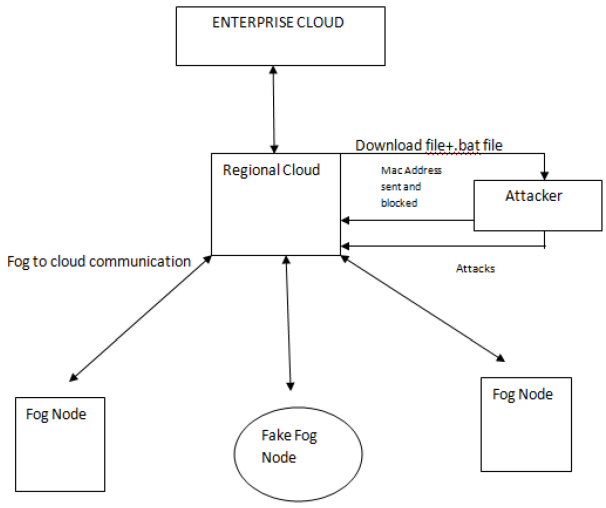

Fig. 4: Proposed Prevention Approach

This approach can theoretically be achieved by using sennaspyoneexemaker software to combine exe file with the hidden batch file and then making user to download and run it. The moment user double clicks it.bat file runs in the background. We can use–arp–a command or any other command to know the mac address of the system and then using redirect command[2] we can save the command in a log.txt file(naming it in such a way that the user does not become suspicious). These all commands and the file will be generated within a few seconds automatically from unauthorised user's point of view. Later we ask the user to upload log.txt in order to proceed further and thus his mac address gets blocked.

A. Future Approach

In future we can design it in a way that we only need to create one fake fog node and according to the traffic this fake node automatically replicates itself making it difficult to identify the location. Furthermore if police can acts the moment the unauthorised user is caught, crime rate will automatically be decreased.

V. CONCLUSION

We have discussed most common security threat to fog computing in this research paper. We have evaluated the Terms and conditions provided by different cloud service providers and have concluded that most of the terms stated are only aiming to steal user's privacy. We have lightened the concepts of data and location privacy and identified new ways the service providers as well as government are misusing. Finally after a depth analysis of common security threat we have proposed a theoretical way of preventing location and data privacy.

REFERENCES

[1] Shanhe Yi, Zhengrui Qin, and Qun Li," Security and Privacy Issues of Fog Computing: A Survey" 2014.

[2] Stojmenovic, I., Wen, S.,"The fog computing paradigm:Scenarios and security issues."In: FedCSIS. IEEE (2014)

[3] Christof Kauba,Stefan Mayer," When the Clouds Disperse Data Confidentiality and Privacy in Cloud Computing" 14. July 2013.

[4] Saniket M. Kudoo, Prof.DilipMotwani," Fog Computing: Data Theft Detection in Cloud with Behaviour Pattern & Decoy Stuff" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 1, January 2016

[5] Salvatore J. Stolfo," Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud", position paper

[6] RajashriRaut,.MadhuriWaje,.Sayali Kulkarni, Ajay K. Gupta," Fog Computing using Advanced Security in Cloud" Vol. 3 Issue 2, February2014.

[7] Kshamata, Prachi, Unathi," Fog Computing Future of Cloud Computing". IJSR(International journal of science and research).

[8] Niranjanamurthi, Kavitha P B." Research study on Fog Computing For secure Data Sercurity" Volume no.5, Special Issue(01), February 2016.

[9] Monjour Ahmed, Mohammad Ashraf Hossain," Cloud Computing and Security issues in the cloud" IJNSA

[10] Kevin Hamlin, Latifur Khan,"Security Issues For Cloud Computing" Technical Report UTDCS-02-10.

[11] K. ChandraHasan," Research Challenges and Security Issues In Cloud Computing" International Journal of Computational Intelligence and Information Security, March 2012 Vol. 3, No. 3.

[12] Osama Harfoushi, Badel Alfawwaz," Data Security Issues and challenges in cloud computing: A conceptual analysis and reviews" vol. 6, No. 1 February 2016.