International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015
ISSN 2091-2730

FOG COMPUTING: REVIEW OF PRIVACY AND SECURITY ISSUES

Neha Shrikant Dhande

Student of Third Year of Computer Engineering,

Shri Sant Gadge Baba College of Engineering and Technology, Bhusawal,

North Maharashtra University, Jalgaon, Maharashtra, India

nehadhande21@gmail.com

Abstract— Fog computing extends cloud computing, cloud computing provide data, compute, storage, and application services to end-user, also the fog computing also provide the services like data, compute ,storage and application to end user. Security and privacy issues are mention in paper. The security solution are available for cloud computing, but they are not useful to fog computing because fog devices working at the edge of the network.

Keywords— cloud computing, fog computing, Man-in-the-Middle Attack, PKI, HAN, WLAN, hijacked.

1. INTRODUCTION

Fog computing is a new standard that exploits the profits of virtualized IT infrastructures closer to end users. In a shell, Fog computing offers an attractive mixture of computational power, storage capability, and networking facilities at the edge of the networks, in Fog computing, facilities can be presented at end devices such as set-top-boxes or access points. The infrastructure of this new scattered computing allows applications to run as close as possible to detected actionable and considerable data, approaching people, methods and thing. Such Fog computing concept, truly a Cloud computing near to the 'ground', creates automated reply that drives the value.

2. SECURITY AND PRIVACY IN FOG COMPUTING

Security Issues

The security issue are authentication at various level of gateways or at the smart meters installed in the customer's home, the ip address has assign to every smart meters or smart appliances, A malicious user can either tamper with its private smart meter, report false readings, or spoof IP addresses. There are some solution should be present for the authentication problem such as public key infrastructure (PKI), another is Diffie-Hellman key exchange [1].

The smart meter encrypt the data and send to the Fog device like a home-area network (HAN) gateway. HAN decrypt data and aggregate the result and pass this decrypt data forward. Intrusion in smart grid can be can be detected using either a signature-based method in this method patterns of behaviour are checked or observed against an already existing database of possible misconducts [7]. Intrusion can also be captured by using an anomaly-based method in which an observed behaviour is compared with expected behavior to check if there is a deviation.

A. An Example: Man-in-the-Middle Attack

Man-in-the-middle attack has potential to become a typical attack in Fog computing. In this part take a Man-in-the-Middle Attack as example to expose security problem in Fog Computing. In this attack the, gateways serving as Fog devices may be compromised or replaced by fake ones. Cases are KFC or Star Bar customers connecting to malicious access points which provide deceptive SSID as public legitimate ones [7]. Attackers take the control of gateways when Private communication of victims will be hijacked.

1) Environment Settings of Stealth Test: Man-in-the-Middle Attack can be very stealthy in Fog computing. Small amount of resources in Fog devices, such as negligible CPU consumption and memory consumption are consumed by this type of attack. Therefore, traditional anomaly detection methods can hardly expose man-in-the-middle attack without noticeable features of this attack collected from the Fog. In order to observe how stealthy the man-in-the-middle attack can be, implement an attack environment displayed in Figure 1[7]. In this section, a 3G user sends a video call to a WLAN user. Since the man-in-the-middle attack needs to control the communication between the 3G user and the WLAN user, the key of this attack is to cooperation the gateway which serves as the Fog device. There are two step to determine the man-in-the-middle attack for the stealth test. First, we need to cooperation the gateway, and second, we insert malicious code into the cooperated system.

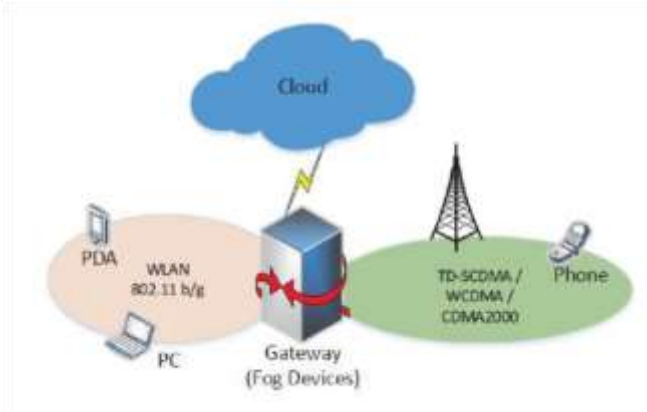

Fig. 1 A scenario for a man-in-the-middle attack towards Fog

2) Work Flow of Man-in-the-Middle Attack*:* Gateway need to translate the data of different protocols into the suitable formats when the 3G and WLAN communicate. Therefore, all the communication data will firstly arrive at the gateway and then be forwarded to other receivers. The man-in-the-middle attack is separated into four steps. The exemplify hijacked communication from 3G to WLAN in Figure 2,the embedded hook process of the gateway redirects the data received from the 3G user to the attacker present in first two process. The attacker replays or modifies the data of the communication at his or her individual computer, and then send the data back to the gateway, and fourth process the gateway forwards the data from the attacker to the WLAN user. In detail, the communication from the WLAN user will also be redirected to the enemy at first, and then be promoted by the hook in the gateway to the 3G user .We can understand noticeably from Figure 2 that the attacker can monitor and modify the data sent from the 3G user to the WLAN user in the 'middle' of the communication**.**

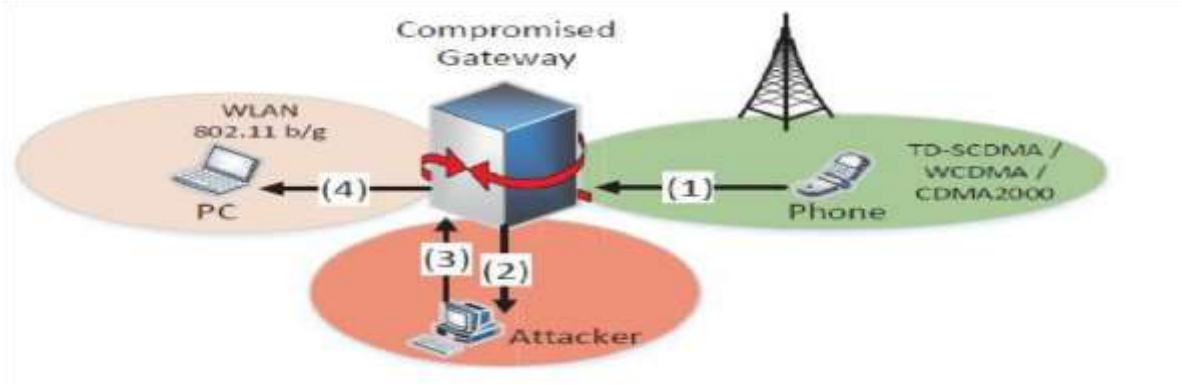

Fig. 2 The hijacked communication in Fog (e.g. from phone to PC)

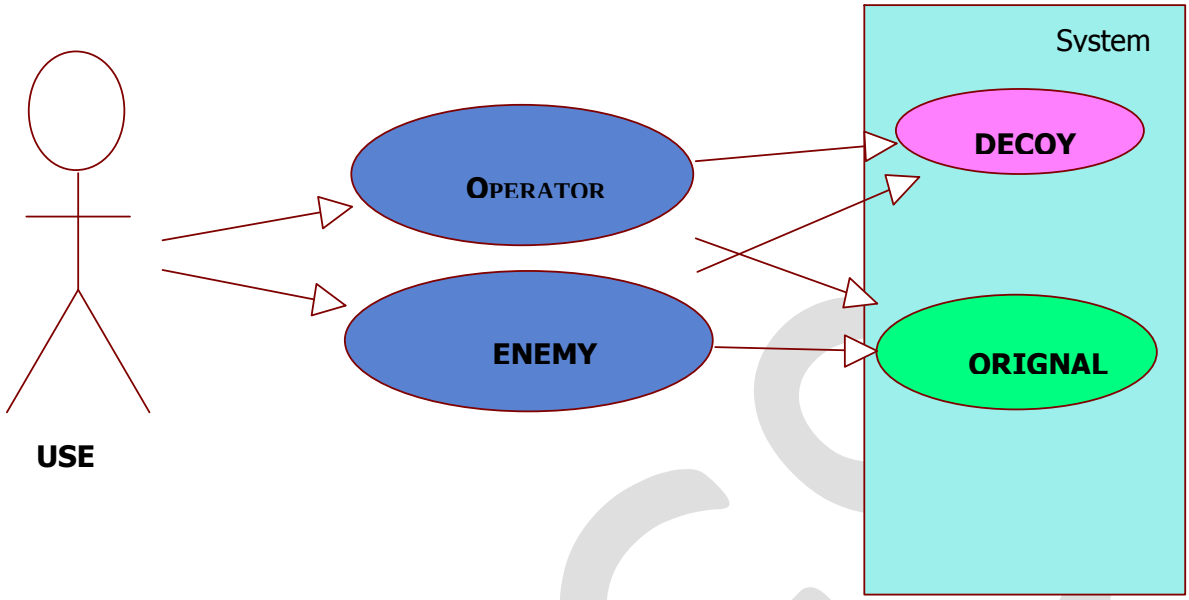

Fig. 3 Decoy System

B. Privacy Issue

In smart grids, privacy issues deal with hiding particulars, such as what appliance was used at what time, while permitting accurate summary information for accurate charging. Described an efficient and privacy-preserving aggregation scheme for smart grid communications [1].The homographic technique used in the privacy issue, a homomorphic function takes as input the encrypted data from the smart meters and produces an encryption [1]. *Ivan Stojmenovic and Sheng Wen* mention their paper that the Fog device cannot decrypt the readings from the smart meter and interfere with them. This ensures the privacy of the data collected by smart meters, but does not promise that the Fog device transmits the correct report to the other gateways.

For data communications from user to smart grid operation center, data aggregation is performed straight on cipher-text at local gateways without decryption, and the aggregation outcome of the original data can be obtained at the operation center [7].Authentication cost is reduced by a batch verification technique

C. Securing Cloud Computing Using Fog Computing

Salvatore J. Stolfo and Malek Ben Salem proposed extra security propose a different approach for securing data in the cloud using offensive decoy technology. By monitoring data access in the cloud detect abnormal data access patterns, and launch a disinformation attack by returning large amounts of decoy information to the attacker. This defends against the misuse of the user's real data.

1) Decoy System-Decoy data, such as decoy documents, honeypots and other fake information can be generated on demand and used for detecting unauthorized access to information and to 'poison' the thief's ex-filtrated information. The Decoy will confuse an attacker into believing they have ex-filtrated valuable information, when they have not. When unauthorized and abnormal access to a cloud facility is noticed, decoy information may be returned by the Cloud and delivered in such a way that it appear completely normal and legitimate. The owner of the information called legitimate user they would readily. We use this technology to launch disinformation attacks against malicious insiders, preventing them from distinctive the real sensitive customer data from fake worthless data the decoys, then, help two purposes:

   (1) Validating whether data access is authorized when abnormal information access is detected.

   (2) Confusing the attacker with fake information.

Applied above concepts to detect unconstitutional data access to data stored on a local file system by attackers who view of legitimate users after stealing their credentials [8].

2) User Behavior Profiling-It is expected that access to a user's information in the Cloud will exhibit a usual resources of access. User profiling is a familiar technique that can be applied here to model in what way, at what time, and how considerable a user accesses their information in the Cloud. Such 'normal user' behaviour can be continuously checked to determine whether abnormal access to a user's information is arising. This method of behaviour-based security is commonly used in fraud detection applications .According to *Salvatore J. Stolfo and Malek Ben Salem*, this is possible pretenses attack. Based on these assumptions they developed the model with the help of one class modelling technique named as one class provision vector machine. Advantage of one class support vector over two class is it has ability of building classifier without sharing data from other users. The privacy of user data is persistent. Investigates done by them indicate that we could reliably detect masquerade attacks using this approach with a very low false positive rate of 1.12% [2]

3. CLOUD Computing VS FOG Computing

Sr.no	**1**	**2**	**3**	**4**	**5**	**6**
Condition	**Latency**	**Delay Jitter**	**No. of server nodes**	**Security**	**Location awareness**	**Support for Mobility**
Cloud Computing	High	High	Few	Undefined	No	Limited
Fog Computing	Low	Very low	Very large	Can be defined	Yes	Supported

ACKNOWLEDGMENT

I would like to thank my honourable Principal Dr. R. P. Singh, my Head of Department, Prof. D. D. Patil, & my special thanks to my class teacher ,prof. R.P. Chaudhari & sincere thanks to prof .L. D. Panjwani and all the respected teaching faculties of department of computer science & engineering. Also I would like to thank my parents, friend for motivating me in this paper work activity. My special thanks to all the writers of reference paper that are referred by me.

CONCLUSION

The author Salvatore J. Stolfo, Malek Ben Salem and Angelos D. Keromytis investigate Fog computing advantages for services in several domains, and provide the analysis security issues in current paradigm**.** Some innovations in compute and storage may be inspired in the future to handle data intensive services based on the interplay between Fog and Cloud.

Future work will expand on the Fog computing paradigm in Smart Grid in this concept two models for Fog devices can be developed. Self-regulating Fog devices consult directly with the Cloud for periodic updates on charge and demands, while connected Fog devices may check each other, and create coalitions for further enhancements.

Fog devices are geographically distributed over diverse platforms. Service mobility across platforms needs to be optimized [1].

REFERENCES:

[1].Ivan Stojmenovic and Sheng Wen, "The Fog Computing Paradigm: Scenarios and Security Issues ", 'IEEE', 2014, Vol. 2, pp. 1–8.

[2].Salvatore J. Stolfo, Malek Ben, Angelos D. Keromytis,"Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud,",'IEEE'.
[3].Mohamed Firdhous, Osman Ghazali and Suhaidi Hassan,"Fog Computing: Will it be the Future of Cloud Computing?",'Third International Conference on Informatics & Applications, Kuala Terengganu, Malaysia, 2014', pp. 8-15.
[4].Prof. Pranalini Joshi and Asavari Smart," Review on Fog computing: Reducing Insiders data theft attack in cloud computing", 'International Journal of Innovative Research in Advanced Engineering (IJIRAE)', 2014, Volume 1 Issue 3, pp.50-53.
[5].Munawar Khatoon,"FOG Computing and Its Role in Internet ",'Internatinal Journal & Magazine of Engineering, Technology, Management and Research ', 2014, Volume No: 4 (2014), pp. 72-74.
[6].Thogaricheti Ashwini, Mrs. Anuradha.S.G,"Fog Computing to protect real and Sensitivity information in Cloud ",' International Journal of Electronics and Computer Science Engineering', pp. 19-29.
[7].V. Anil Kumar, E.Prasad,"Fog Computing: Characteristics, Advantages and Security-Privacy", 'International Journal of Computer Science and. Management Research', 2014, VOL 3, pp.4212-4215.
[8]Tom H. Luan, Longxiang Gao, Yang Xiang and Zhi Li, Limin Sun, "Fog Computing: Focusing on Mobile Users at the Edge",'arXiv', 6 Feb 2015.

IJERGS