ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

Edge Computing Under Security Concerns

S.Umadevi@Yashodei, S.Kiruthika, S.Ashimabanu, R.Dhaarani,

Assistant Professor, Dept. of ECE, IFET College of Engineering, Villupuram, Tamil Nadu, India

UG Student, Dept. of ECE, IFET College of Engineering, Villupuram, Tamil Nadu, India

UG Student, Dept. of ECE, IFET College of Engineering, Villupuram, Tamil Nadu, India

UG Student, Dept. of ECE, IFET College of Engineering, Villupuram, Tamil Nadu, India

ABSTRACT: Fog Computing is also said to be as a edge computing and it is a paradigm that extends Cloud computing and services to the edge of the network. Similar to Cloud, Fog provides data, compute, storage, and application services to end-users. In this article, we elaborate the motivation and advantages of Fog computing, and analyze its applications in a series of real scenarios, such as Smart Grid, smart traffic lights in vehicular networks and software defined networks. Security and privacy issues are further disclosed according to current Fog computing paradigm. As an example, we study a typical attack, man-in-the-middle attack, for the discussion of security in Fog computing. We investigate the stealthy features of this attack by examining its CPU and memory consumption on Fog device.

KEYWORDS: Fog Computing, Cloud Computing, Internet of Things, Software Defined Networks.

I. INTRODUCTION

CISCO recently delivered the vision of fog computing to enable applications on billions of connected devices, already connected in the Internet of Things (IoT), to run directly at the network edge [1]. Customers can develop, manage and run software applications on Cisco I Ox framework of networked devices, including hardened routers, switches and IP video cameras. Cisco I Ox brings the open source Linux and Cisco IOS network operating system together in a single networked device (initially in routers). The open application environment encourages more developers to bring their own applications and connectivity interfaces at the edge of the network. Regardless of Cisco‟s practices, we first answer the questions of what the Fog computing is and what are the differences between Fog and Cloud. Both Cloud and Fog provide data, computation, storage and application services to end-users. We adopt a simple three level hierarchy as in Figure 1. In this framework, each smart thing is attached to one of Fog devices. Fog devices could be interconnected and each of them is linked to the Cloud.

In this article, we take a close look at the Fog computing paradigm. The goal of this research is to investigate Fog computing advantages for services in several domains, such as Smart Grid, wireless sensor networks, Internet of Things (IoT) and software defined networks (SDNs). We examine art the state-of-the- and disclose some general issues in Fog computing including security, privacy, trust, and service migration among Fog devices and between Fog and Cloud. We finally conclude this article with discussion of future work

II. WHY DO WE NEED FOG?

In the past few years, Cloud computing has provided many opportunities for enterprises by offering their customers a range of computing services. Current “pay-as-you-go” Cloud computing model becomes an efficient alternative to owning and managing private data centers for customers facing Web applications and batch processing [3]

Cloud computing frees the enterprises and their end users from the specification of many details, such as storage resources, computation limitation and network communication cost. However, this bliss becomesa problem for latency-

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

sensitive applications, which require nodes in the vicinity to meet their delay requirements [2]. When techniques and devices of IoT are getting more involved in people‟s life, current Cloud computing paradigm can hardly satisfy their requirements of mobility support, location aware-ness and low latency.

III. WHAT CAN WE DO WITH FOG?

We elaborate on the role of Fog computing in the following six motivating scenarios. The advantages of Fog computing satisfy the requirements of applications in these scenarios.
Smart Grid: Energy load balancing applications may run on network edge devices, such as smart meters and micro-grids [4]. Based on energy demand, availability and the lowest price, these devices automatically switch to alternative energies like solar and wind. As shown in Figure 2, Fog collectors at the edge process the data generated by grid sensors and devices, and issue control commands to the actuators [2]. They also filter the data to be consumed locally, and send the rest to the higher tiers for visualization, real-time reports and transactional analytics. Fog supports ephemeral storage at the lowest tier to semi-permanent storage at the highest tier. Global coverage is provided by the Cloud with business intelligence analytics.

Smart Traffic Lights and Connected Vehicles: Video cam-era that senses an ambulance flashing lights can automatically change street lights to open lanes for the vehicle to pass through traffic. Smart street lights interact locally with sensors and detect presence of pedestrian and bikers, and measure the distance and speed of approaching vehicles. As shown in Figure 3, intelligent lighting turns on once a sensor identifies movement and switches off as traffic passes. Neighboring smart lights serving as Fog devices coordinate to create green traffic wave and send warning signals to approaching vehicles [2]. Wireless access points like Wi-Fi, 3G, road-side units and smart traffic lights are deployed along the roads. Vehicles-to-Vehicle, vehicle to access points, and access points to access points interactions enrich the application of this scenario.

Wireless Sensor and Actuator Networks: Traditional wire-less sensor networks fall short in applications that go beyond sensing and tracking, but require actuators to exert physical actions like opening, closing or even carrying sensors [2].
.
Decentralized Smart Building Control: The applications of this scenario are facilitated by wireless sensors deployed to measure temperature, humidity, or levels of various gases in the building atmosphere. In this case, information can be exchanged among all sensors in a floor, and their readings can be combined to form reliable measurements. Sensors will use distributed decision making and activation at Fog devices to react to data.

The system components may then work together to lower the temperature, inject fresh air or open windows. Air conditioners can remove moisture from the air or increase the humidity. Sensors can also trace and react to movements (e.g, by turning light on or off). Fog devices could be assigned at each floor and could collaborate on higher level of actuation. With Fog computing applied in this scenario, smart buildings can maintain their fabric, external and internal environments to conserve energy, water and other resources.

Software Defined Networks (SDN): As shown in Figure 6, Fog computing framework can be applied to implement the SDN concept for vehicular networks. SDN is an emergent computing and networking paradigm, and became one of the most popular topics in IT industry [7]. It separates control and data communication layers. Control is done at a centralized server, and nodes follow communication path decided by the server. The centralized server may need distributed implementation. SDN concept was studied in WLAN, wireless sensor and mesh networks, but they do not involve multi-hop wireless communication, multi-hop routing.

Smart Parking Deployment :
Parking Sensors are deployed on the curb in all the streets of the pilot area (reliability of car detection is over 97%) . Parking spaces are marked with numbers.Multi-Services kiosks are deployed on the streets.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

Smart Mobility: EzPark: Real-time info about parking availability. Real-time and Predictive Traffic** information including itinerary calculation . Real-time info about parking pricing . Pay ByPhone/NFC payment Impact . Parking commuters benefit from time saving for a search and easier way to manage overall transportation means

EzMove:
Real-time Information about public and electric car sharing service (itinerary calculation) . Booking service for electric car sharing .NFC Payment for electric car sharing

EzCity :
On going creation of e-Service to inform users (managed by the City) .Retailer couponing and deals**

Street Light Management :
Lamp intensity monitored according to information sent by luminosity & traffic sensors. Diverse sensors taking into account multiple criteria: natural light (day or night), weather conditions (eg: more light in the event of fog), presence of cars (Light substitute with car headlight), presence of physical persons (less light in case of higher concentration of persons and more light in the event of an isolated person) .Match comfort and security dimensions .

Street Lighting Evolution :
Beyond smart LED, city leaders and street lighting vendor are envisioning street light as a multi service platform . Street lights are everywhere and once connected to power and network they could host many services: sensors, wireless transceiver (wifi, PAN, small cell), digital signs, communication . Philips (e.g. Barcelona) and others are leading the initiative .However average lifespan of street light pole is 30 to 40 years. Replacing all light pole with next-generation street light is a long term process.

The fog computing environment which represents the smart applications on itself. In which the cities has based on their smart applications towards on its new technology.

A.Related Work
K. Hong et al. proposed mobile Fog in [1]. This is a high level programming model for geo-spatially distributed, large-scale and latency-sensitive future Internet applications. Following the logical structure shown in Figure 1, low-latency processing occurs near the edge while latency-tolerant large-scope aggregation is performed on powerful resources in the core of the network (normally the Cloud). Mobile Fog consists of a set of event handlers and functions that an application can call. Mobile Fog model is not presented as generic model, but is built for particular application, while leaving out functions that deal with technical challenges of involved image processing primitives. Fog computing approach reduces latency and network traffic.

B.Similar Work
BETaaS [1] proposed replacing Cloud as the residen-t for machine-to-machine applications by „local Cloud‟ of gateways. The „local Cloud‟ is composed of devices that provide smart
things with connectivity to the Internet, such as smart phones, home routers and road-side units. This enables applications that are limited in time and space to require simple and repetitive interactions. It also enables the applications to respond in consistent manner.

The main drawback of this algorithm is a significant communication overhead between users and utility companies. Though DRM helps to facilitate the reliability of power supply, the smart grid can be susceptible to privacy and security issues because of communication links between the utility companies and the consumers. They study the impact of an attacker who can manipulate the price information from the utility companies, and propose a scheme based on the concept of shared reserve power to improve the grid reliability and ensure its dependability.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

IV. SECURITY AND PRIVACY IN FOG COMPUTING

Security and privacy issues were not studied in the context of fog computing. They were studied in the context of s-mart grids [24] and machine-to-machine communications [25].
Fig.10.Thw internet of Things Architecture and Fog computing
There are security solutions for Cloud computing. However, they may not suit for Fog computing because Fog devices work at the edge of networks. The working surroundings of Fog devices will face with many threats which do not exist in well managed Cloud. In this section, we discuss the security and privacy issues in Fog Computing.

A. Security Issues
The main security issues are authentication at different levels of gateways as well as (in case of smart grids) at the smart meters installed in the consumer‟s home. Each smart meter and smart appliance has an IP address. A malicious user can either tamper with its own smart meter, report false readings, or spoof IP addresses. There are some solutions for the authentication problem. The work [6] elaborated public key infrastructure (PKI) based solutions which involve multicast authentication. Some authentication techniques using Diffie-Hellman key exchange have been discussed in [7]. Smart meters encrypt the data and send to the Fog device, such as a home-area network (HAN) gateway. HAN then decrypts the data, aggregates the results and then passes them forward. Intrusion detection techniques can also be applied in Fog computing [8]. Intrusion in smart grids can be detected using either a signature-based method i in which the patterns of behaviour are observed and checked against an already existing database

Intrusion can also be captured by using an anomaly-based method in which an observed behaviour is compared with expected behaviour to check if there is a deviation. The work [9] develops an algorithm that monitors power flow results and detects anomalies in the input values that could have been modified by attacks. The algorithm detects intrusion by using principal component analysis to separate power flow variability into regular and irregular subspaces.

B. An Example: Man-in-the-Middle Attack
Man-in-the-middle attack has potential to become a typical attack in Fog computing. In this subsection, we take man-in-the- middle attack as an example to expose the security problems in Fog computing. In this attack, gateways serving as Fog devices may be compromised or replaced by fake ones [30]. Examples are KFC or Star Bar customers connecting to malicious access points which provide deceptive SSID as public legitimate ones.

1) Environment Settings of Stealth Test: Man-in-the-middle attack can be very stealthy in Fog computing paradigm. This type of attack will consume only a small amount of resources in Fog devices, such as negligible CPU utilization and memory consumption. 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 examine how stealthy the man-in-the-middle attack can be, we implement an attack environment shown in Figure 5. In this scenario, a 3G user sends a video call to a WLAN user. Since the man-in-the-middle attack requires to control the communication between the 3G user and the WLAN user, the key of this attack is to compromise the gateway which serves as the Fog device.
Two steps are needed to realize the man-in-the-middle attack for the stealth test. First, we need to compromise the gateway, and second, we insert malicious code into the compromised system. For susceptible gateways, we can either refresh the ROM of a normal gateway or place a fake active point.

2) Work Flow of Man-in-the-Middle Attack: The communication between 3G and WLAN needs a gateway to translate the data of different protocols into the suitable formats. Therefore, all the communication data will firstly arrive at the gateway and then be forwarded to other receivers.
In our experiment, the man-in-the-middle attack is divided into four steps. We illustrate the hijacked communication from 3G to WLAN in Figure 7. In the first two steps, the embedded hook process of the gateway redirects the data received from the 3G user to the attacker. The attacker replays or modifies the data of the communication at his or her own computer, and then send the data back to the gateway. In the final step, the gateway forwards the data from the

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

attacker to the WLAN user. In fact, the communication from the WLAN user will also be redirected to the attacker at first, and then be forwarded by the hook in the gateway to the 3G user.

3) Results of Stealth Test: Traditional anomaly detection techniques rely on the deviation of current communication from the features of normal communication. These features include memory consumption, CPU utilization, bandwidth usage, etc. Therefore, to study the stealth of man-in-the-middle attack, we examine the memory consumption and the CPU utilization of gateway during the attack. If man-in-the-middle attack does not greatly change the features of the communication, it can be proofed to be a stealthy attack. For simplicity, we assume the attacker will only replay the data at his or her own computer but will not modify the data.
Firstly, we compare the memory utilization of gateway before and
after a video call tunnel is built in our experiment.
The results are shown in Figure 8, and the red line in plots indicates the average amount of memory consumption. We can see clearly that man-in-the-middle attack does not largely influence the video communication.

C. Privacy Issues
In smart grids, privacy issues deal with hiding details, such as what appliance was used at what time, while allowing correct summary information for accurate charging. R. Lu et al. described an efficient and privacy-preserving aggregation scheme for smart grid communications . It uses a super-increasing sequence to structure multi-dimensional data and encrypt the structured data by the homo-morphic cryptogram technique. A homo-morphic function takes as input the encrypted data from the smart meters and produces an encryption of the aggregated result. The Fog device cannot decrypt the readings from the smart meter and tamper with them. This ensures the privacy of the data collected by smart meters, but does not guarantee that the Fog device transmits the correct report to the other gateways.

V. PROPOSED APPROACH IN CRYPTOGRAPHY

Attacker Victims

Hook AMRH.263 H.324M
Process
IP_INPUT Linux IP StackIP_OUTPUT

The existing techniques involve the use of keys involving Prime numbers and the like. As a step further ahead let us considers a technique in which we use prime numbers under the Fibonacci concepts and colors. Further we also use a combination of substitution and permutation methods to ensure data security. We perform the substitution process by assigning the ASCII equivalent to the characters. Permutation process is performed by using matrices as in [2] and prime numbers in Fibonacci .In this technique the first step is to assign a unique color for each receiver. Each color is represented with a set of three values. For example violet red color is represented in RGB format as (238, 58,140). The next step is to assign a set of three key values to each receiver.

The above technique involves keys with a minimum length of 8 bits for Prime numbers. This minimum key length reduces the efforts taken to encrypt the data. The key length can be increased if needed, with increase in character length. This increases the complexity thereby providing increased security. This technique ensures that the data transfer can be performed with protection since it involves two main steps. First step is to convert the characters into another form, by adding with the digits of the Prime numbers. Second step is to encode using a matrix to form the required encrypted data. Tracing process becomes difficult with this technique. This is because the Prime numbers is used differently in each step. The key can be hacked only if the entire steps involved in the encoding process are known earlier. This technique could be considered as a kind of triple DES algorithm since we use three different keys namely the colors, key values added with the colors and prime numbers. Unless all the three key values along with the entire encryption and decryption technique is known the data cannot be obtained. So hacking becomes difficult mainly because of the usage of colors. Simple encryption and decryption techniques may just involve encoding and decoding

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

the actual data. But in this proposed technique the password itself is encoded for providing more security to the access of original data.

VI. CONCLUSIONS AND FUTURE WORK

We investigate Fog computing advantages for services in several domains, and provide the analysis of the state-of-the-art and security issues in current paradigm. Based on the work of this paper, 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 scenario, two models for Fog devices can be developed. Independent Fog devices consult directly with the Cloud for periodic updates on price and demands, while interconnected Fog devices may consult each other, and create coalitions for further enhancements. Next, Fog computing based SDN in vehicular networks will receive due attention. For instance, an optimal scheduling in one communication period, expanded toward all communication periods, has been elaborated in [6]. Traffic light control can also be assisted by the Fog computing concept. Finally, mobility between Fog nodes, and between Fog and Cloud, can be investigated. Unlike traditional data centres, Fog devices are geographically distributed over heterogeneous platforms.

REFERENCES

[1]F. Bonomi, "Connected vehicles, the internet of things, and fog com-puting," in The Eighth ACM International Workshop on Vehicular Inter-Networking (VANET), Las Vegas, USA, 2011.
[2]F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in Proceedings of the First Edition ofthe MCC Workshop on Mobile Cloud Computing, ser. MCC″12. ACM,2012, pp. 13–16.
[3]M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr 2010.
[4]C. Wei, Z. Fadlullah, N. Kato, and I. Stojmenovic, "On optimally reducing power loss in micro-grids with power storage devices," IEEEJournal of Selected Areas in Communications, 2014 to appear.
[5]L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct. 2010.
[6]K. Liu, J. Ng, V. Lee, S. Son, and I. Stojmenovic, "Cooperative data dissemination in hybrid vehicular networks: Vanet as a software defined network," Submitted for publication, 2014.
[7]K. Kirkpatrick, "Software-defined networking," Commun. ACM, vol. 56, no. 9, pp. 16–19, Sep. 2013.
[8]Cisco, "Cisco delivers vision of fog computing to accelerate value from billions of connected devices," Cisco, Tech. Rep., Jan. 2014.
[9]K. Hong, D. Lillethun, U. Ramachandran, B. Ottenwälder, and B. Kold-ehofe, "Opportunistic spatio-temporal event processing for mobile situation awareness," in Proceedings of the 7th ACM International Confer-ence on Distributed Event- based Systems, ser. DEBS″13. ACM, 2013,pp. 195–206.