Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Fog Computing: Security in Cloud Environment

Divya Shrungar J, Priya M P, Asha S M
M.Tech, Dept. of CSE
India

Abstract-The distributed computing attempts to improve performance in large-scale computing problems by resource sharing. Moreover, rising low-cost computing power coupled with advances incommunications/networking and the advent of big data, now enables new distributed computing paradigms such as Cloud, and Fog computing. Cloud Computing provides us a means of accessing the utilities as applications through internet. The users are provided with on-demand resources for their organizations. Although Cloud Computing increases the performance it also has some downsides like data theft and various attacks. This enables the intruder for the misuse of data and also interpretation of highly confidential data for illegal purpose. For securing user data from such attacks a new paradigm called Fog Computing. This can monitor the user activity to identify the legitimate access and prevent from any unauthorized access of data. In this paper we have discussed about Fog Computing for preventing misuse of user data and provide security.

Keywords: Distributed computing; Cloud computing; Fog computing.

I. INTRODUCTION

Nowadays Cloud computing is achieving popularity because of its ease of usage and storage which is provided to users for personal and business purposes is increasing its demand. It is a well-situated, on- demand access to a shared pool of resources [1]. Business agencies and software companies are admiring cloud computing for its elasticity and ease of access. For attaining more and more operational efficiency and managing data organization with small or large businesses are using cloud environments. Cloud computing is a combination of service oriented architecture and many computing strategies such as virtualization, multitenancy, elasticity, service-oriented architecture, and resource pooling. The development of Cloud computing technology faced many critical obstacles such as security, availability, accountability, confidentiality, privacy, data provenance, data lock-in, Cloud interoperability, lack of standardization, SLA issues, customization, performance unpredictability, technology bottlenecks, etc., which are addressed in many researches. Very common risk nowadays in geographical distributed cloud environment is data theft. It is considered as one of the top threats to user data in cloud environment [2]. To overcome this threat a mechanism is required which can detect the malicious activities. Fog computing is such a paradigm which helps in monitoring and identifying the unauthorized accesses. According to Cisco, Fog computing is well suited for geographical distributed cloud environment to provide security. Fog nodes provide localization, therefore enables low latency and context awareness, the cloud provides global centralization [3]. Fog computing involves a dense geographical distribution of network and provides a feature of location access. By this any malicious activity in the cloud network can be detected. The application built for solving the problem of data theft includes a mechanism which audits the user behavior. The common notation of a cloud insider as a rouge administrator of service provider, but there are also two additional cloud related insider risks: 1) The insider who exploits a cloud-related vulnerabilities to get the information from cloud based systems, and 2) The insider who exploits the cloud systems and carry out attack on an employer's local resource [4].

II. WHAT IS FOG COMPUTING?

The term Fog computing has been embraced by Cisco Systems as a new paradigm. Fog computing is a systematic, highly virtual, secure, and network-integrated platform that provides computing, storage, and networking services between end points and traditional Cloud computing data centers. It is a paradigm in which data, processing and applications are concentrated in devices at the network edge, rather than existing almost entirely in the Cloud, to isolate them from the Cloud systems and place them closer to the end-user, which is the aim of Fog computing [5].

III. WHY DO WE NEED FOG?

As Fog computing is implemented at the edge of the network, it provides low latency, location awareness, and improves quality-of-services (QoS) for streaming and real time applications. Typical examples include industrial automation, transportation, and networks of sensors and actuators. Moreover, this new infrastructure supports heterogeneity as Fog devices include end-user devices, access points, edge routers and switches. The Fog paradigm is well suited for real time big data analytics, supports densely distributed data collection points, and provides advantages in entertainment, advertising, personal computing and other applications.

IV. WHAT CAN WE DO WITH FOG?

The advantages of Fog computing satisfy the requirements of applications in these scenario

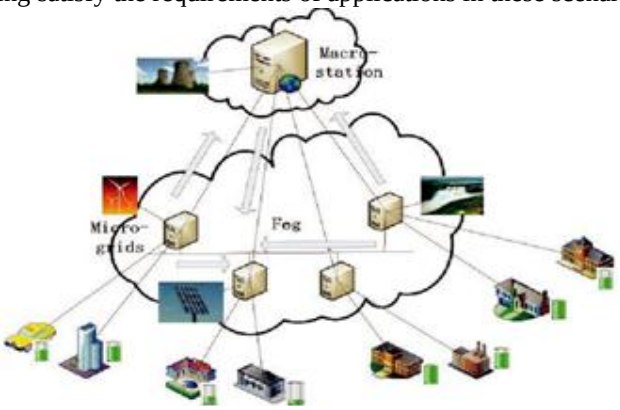

Fig-1: Fog computing in smart Grid.

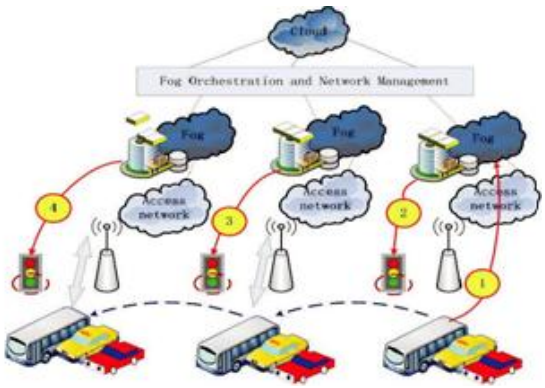

Fig-2: Fog computing in Smart Traffic lights and connected vehicles.

Smart Grid: Energy load balancing applications may run on network edge devices, such as smart meters and micro-grids [15]. 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 [14]. 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.Fig.2. Fog computing in smart traffic lights and connected vehicles.

Smart Traffic Lights and Connected Vehicles: Video camera 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 [14]. Wireless access points like WiFi, 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 wireless 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 [14]. In this scenario, actuators serving as Fog devices can control the measurement process itself, the stability and the oscillatory behaviors by creating a closed-loop system. For example, in the scenario of self-maintaining trains, sensor monitoring on a train's ball-bearing can detect heat levels, allowing applications to send an automatic alert to the train operator to stop the train at next station for emergency maintenance and avoid potential derailment. In lifesaving air vents scenario, sensors on vents monitor air conditions flowing in and out of mines and automatically change air-flow if conditions become dangerous to miners.

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**.**

IoT and Cyber-physical systems (CPSs): Fog computing based systems are becoming an important class of IoT and CPSs. Based on the traditional information carriers including Internet and telecommunication network, IoT is a network that can interconnect ordinary physical objects with identified addresses [13]. CPSs feature a tight combination of the system's computational and physical elements. CPSs also coordinate the integration of computer and information centric physical and engineered systems. IoT and CPSs promise to transform our world with new relationships between computer-based control and communication systems, engineered systems and physical reality. Fog computing in this scenario is built on the concepts of embedded systems in which software programs and computers are embedded in devices for reasons other than computation alone. Examples of the devices include toys, cars, medical devices and machinery. The goal is to integrate the abstractions and precision of software and networking with the dynamics, uncertainty and noise in the physical environment. Using the emerging knowledge, principles and methods of CPSs, we will be able to develop new generations of intelligent medical devices and systems, 'smart' highways, buildings, factories, agricultural and robotic systems. **Software Defined Networks (SDN):** As shown in Figure 4, 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 [11]. 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 multihop wireless communication, multi-hop routing. Moreover, there is no communication between peers in this scenario. SDN concept together with Fog computing will resolve the main issues in vehicular networks, intermittent connectivity, collisions and high packet loss rate, by augmenting vehicleto-vehicle with vehicle-to-infrastructure communications and centralized control. SDN concept for vehicular networks is first proposed in [10].

V. ARCHITECTURE OF FOG COMPUTING

Fog computing is well suited for the geographical distribution of resources instead of having a centralized one, meaning Fog computing is the extension of Cloud computing. The difference is Fog provides proximity to its end users through dense geographical distribution and it also supports mobility. Access points or set-up boxes are used as end devices to host services at the network. In Fog computing platform multi-tier architecture is used. In first tier there is machine to machine communication and the higher tiers deals with visualization and reporting. The higher tier is represented by the cloud. The architecture is as shown in the fig.1 shown below.

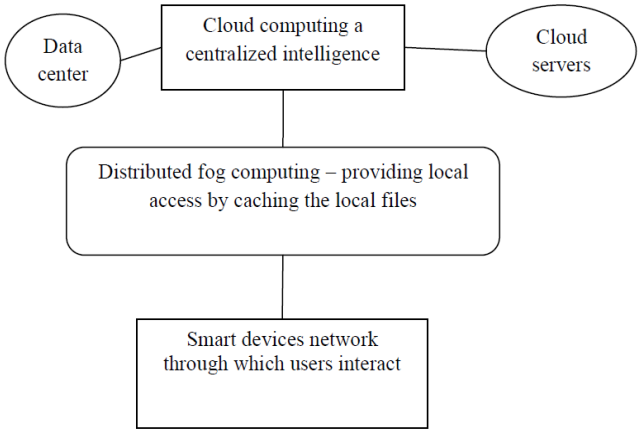

Fig-3: Architecture of Fog computing

Z. Jiang et al. [6] Discussed Fog computing architecture and future used it for improving Web site's performance with the help of edge servers. They have explained that the emerging architecture of Fog computing is highly virtualized. They presented that their idea that the Fog servers monitor the requests made by the users and keep a record of each request by using the user's IP address or MAC address.

VI. CHALLENGES IN FOG COMPUTING

There are many open problems that will have to be addressed to make the fog a reality [7]. It is necessary to clearly identify these problems so future research works can focus on them. The set of open challenges for the fog to become a reality is:

1) Discovery/Sync: Applications running on devices may need either some agreed 'centralized' point (e.g. establish an "upstream" backup if there are too few peers in our storage application);

***2) Compute/Storage limitation*:** Current trends are improving this fact with smaller, more energy-efficient and more powerful devices (e.g. one of today's phones is more powerful than many high end desktops from 15 years ago). Still new improvements are granted for non consumer devices;

***3) Management* :** In addition to setting up the communication routes across end nodes, IoT/ubiquitous computing nodes and applications running on top need to be properly setup and configured to operate as desired. Having potentially billions of small devices to be configured, the fog will heavily rely on decentralized (scalable) management mechanisms

that are yet to be tested at this unprecedented scale. One thing that can be predicted with certain degree of confidence is that there will be no full control of the whole fog and asymptotic declarative configuration techniques will become more common;

***4) Security*:** The same security concerns that apply to current virtualized environments can be foreseen to affect fog devices hosting applications. The presence of secure sandboxes for the execution of droplet applications poses new interesting challenges: Trust and Privacy. Before using other devices or mini-clouds in the network to run some software, isolation and sandboxing mechanisms must be in place to ensure bidirectional trust among cooperating parties. The fog will allow applications to process user's data in thirdparty's hardware/software. This of course introduces strong concerns about data privacy and its visibility to those thirdparties;

***5) Standardization*:** Today no standardized mechanisms are available so each member of the network (terminal, edge point...) can announce its availability to host others' software components, and for others to sent it their software to be run;

***6) Accountability/Monetization*:** Enabling users to share they spare resources to host applications is crucial to enable new business models around the concept of the fog. A proper system of incentives needs to be created. The incentives can be financial or otherwise (e.g. unlimited free data rates). On the other hand the lack of central controlling entity in the fog makes it difficult to assert if a given device is indeed hosting a component (droplet) or not;

***7) Programmability*:** Controlling application lifecycle is already a challenge in cloud environments [8]. The presence of small functional units (droplets) in more locations (devices) calls for the right abstractions to be in place, so that programmers do not need to deal with these difficult issues [9]. Easy to use APIs for programmers will heavily rely on simple *Management* mechanisms that provide them with the right abstractions to hide the massive complexity of the fog. Some vendors like Microsoft have already taken some steps in positioning themselves in this space9. Table 2 discusses which of these challenges are inherently new and which ones have been inherited by the fog from one of its "parent" technologies.

VII. CONCLUSION AND FUTURE WORK

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 [11]. 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 centers, Fog devices are geographically distributed over heterogeneous platforms. Service mobility across platforms needs to be optimized.

REFERENCES

[1] Hashizume K., Rosado D. G., Fernandez- Medina E. and Fernandez E. B."An analysis of security issues for cloud computing". Journal of Internet Services and Applications, 2013, 4(1), pp.1-13.

[2] Archer, Jerry,l. "Top threats to cloud computing v1. 0."Cloud Security Alliance, 2010.

[3] Bonomi, Flavio, et al. "Fog Computing And Its role in the Internet of Things." Proceedings of the first edition of the MCC workshop on Mobile cloud computing. ACM, 2012, pp.13-16.

[4] Park, Y., & Stolfo, S. J. "Software decoys for insider threat", In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, 2012, May, pp. 93-94.

[5] Majid Hajibaba and Saeid Gorgin "A Review on Modern Distributed Computing Paradigms: Cloud Computing, Jungle Computing and Fog Computing" Journal of Computing and Information Technology - CIT 22, 2014, 2, 69–84.

[6] Zhu, Jiang, "Improving Web Sites Performance Using Edge Servers in Fog Computing Architecture", Service Oriented System Engineering (SOSE), IEEE. 2013.

[7] Luis M. Vaquero and Luis Rodero-Merino "Finding your Way in the Fog: Towards a Comprehensive Definition of Fog Computing" ACM SIGCOMM Computer Communication Review - Volume 44, Number 5, October 2014.

[8] Luis M. Vaquero, Daniel Mor´an, Ferm´ın Gal´an, and Jose M. Alcaraz-Calero. Towards runtime reconfiguration of application control policies in the cloud. *J. Netw. Syst. Manage.*, 20(4):489–512, December 2012. ACM.

[9] Kirak Hong, David Lillethun, Umakishore Ramachandran, Beate Ottenw¨alder, and Boris Koldehofe. Mobile fog: A programming model for large-scale applications on the internet of things. In *Proceedings of the Second ACM SIGCOMM Workshop on Mobile Cloud Computing*, MCC '13, pages 15–20, New York, NY, USA, 2013. ACM.

[10] F. Bonomi, "Connected vehicles, the internet of things, and fog computing," in The Eighth ACM International Workshop on Vehicular InterNetworking (VANET), Las Vegas, USA, 2011.

[11] 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.

[12] K. Kirkpatrick, "Software-defined networking," Commun. ACM, vol. 56, no. 9, pp. 16–19, Sep.2013.

[13] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct.2010.

[14] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the FirstEdition of the MCC Workshop on Mobile Cloud Computing*, ser. MCC'12. ACM, 2012, pp. 13–16.

[15] C. Wei, Z. Fadlullah, N. Kato, and I. Stojmenovic, "On optimally reducing power loss in micro-grids with power storagedevices," *IEEE Journal of Selected Areas in Communications*, 2014 to appear.

