Preventing Insider Data Theft Attacks in the Cloud using Fog Computing the Cloud

Ragam Kedarnath[1], Firoze Pattan[2]
[1] *P.G. Scholar,* [2] *Assoc. Professor*
[1, 2] *Department of CSE, GVR & S College of Engineering & Technology, Guntur, A.P., India*

Abstract **-** In large-scale IoT applications, Fog computing is an evolving technology to tackle computing and networking bottlenecks. The computer model for cloud computing is a promising one, where computer, networking, storage and acceleration components are multi-leveled, distributed and likely collaborative on the borders and network layers. These elements may include virtualized computing features on edge devices or network elements that apply the computing principle everywhere. This paper presents an integrated taxonomy for the architectural, algorithmic and technological dimensions of fog computing to bring current research in perspective. The computing paradigms, including cloud, edge, mobile edge and fog computing, are subsequently reviewed and their architectural distinctions. Practical use of fog computing involves a variety of aspects, including system design, application design, implementation of software, security, management of computer resources, and networking. An extensive architectural survey of all these aspects is included. Present architectures and software detailing their excellent features and variations in fog-computing are being studied. Basis Architectures are presented and analyzed using a proposed maturity model for applications, software, security, resource management and networking.

Keywords: Cloud computing, Security, User profiling behavior, Decoy technology

I. INTRODUCTION

As virtualization technologies mature and are pervasively adopted, multi-tenancy is becoming possible not only in high-end computing servers but also in network elements and even end-user equipment. Thus, there is a trend towards creating network and user functions as virtual functions that are outsourced for execution in utility-based computing stores. This trend is driven by the emergence of universal composability that transforms monolithic applications into composable micro-services.

The tasks and the associated micro-services vary widely in their requirements, including computing resources, elasticity, interactivity, and latency. These developments have given new life to the concept of ubiquitous computing and the notion of computing everywhere. In this new environment, each and every computing resource may be selected as the best match for some virtual functions or tasks because of location, resources and requirements. Fog computing provides a framework for task segmentation, placement, offloading and execution in a distributed and collaborative environment and hence will play a major role in this new age of computing.

Cloud computing plays the leading role to provide on demand location-independent computing services in cloud data centers that may be quite distant from the user. However, with the advent and widespread adoption of cloud computing, many new dimensions have been introduced to adapt it to the needs of various computing paradigms. Multi-tier cloud computing, edge computing, mobile edge computing and more recently fog computing are among the complementary trends emerged to help optimize resource utilization and to meet application requirements.

A number of features in cloud computing can be seen in Figure 1. However, most of the Cloud data centres are situated in remote areas, a long way from the end-proximity. user's As a result, in many cases reliable requests for a computing service, in real-time and latency, suffer significant delays, network congestion, and loss of service quality. Figure 1 illustrates multiple problems in nutshell with cloud computing.

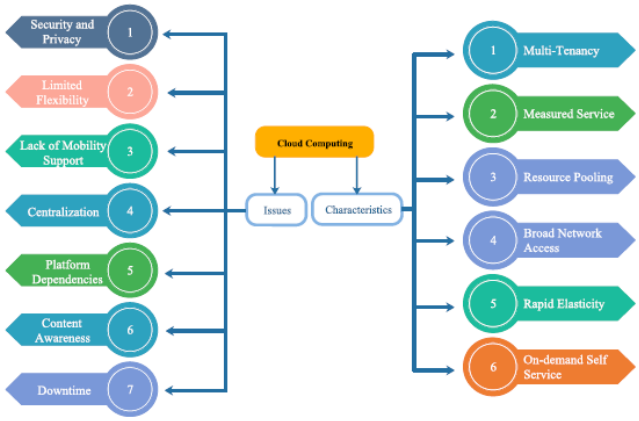

Figure 1. Cloud computing characteristics and issues.

Fog computing aims at supporting applications that cannot effectively support cloud-based solutions with poor

latency, geo-distributing, position consciousness and distributed controlling. Fog nodes are heterogeneous and are used in different areas, such as heart, edge and access networks. The management of fog resources is needed to ensure the smooth management of resources across the various platforms. In order to host a variety of applications, including vehicle networks and IoT applications, Fog architecture should also be versatile enough. Figure 2 illustrates the complex cisco architecture.

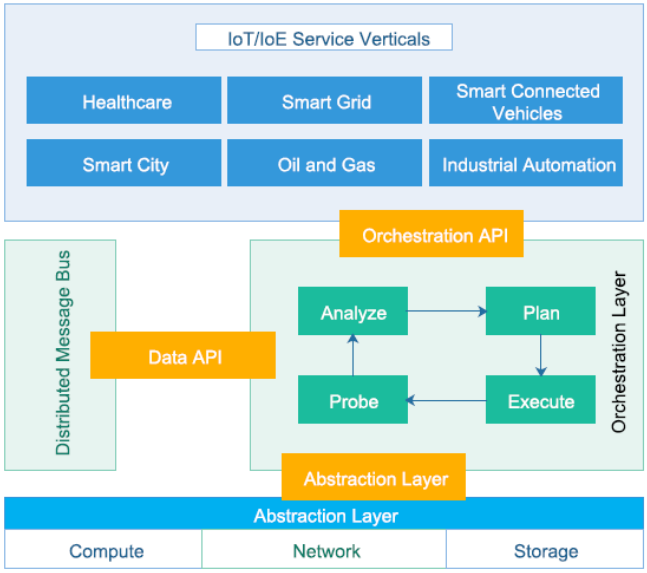

Figure 2. Cisco-Bonomi reference architecture

II. RELATED WORK

Fog computing presents a new computing paradigm where computation capability, storage capacity, and networking services are placed at the edge and/or in the network, rather than in the cloud over the Internet [1], [2]. Furthermore, management of computing, networking, and storage facilities and programming of networking resources is made possible in a harmonized coordinated manner in fog computing [3], [4]. It provides a ubiquitous and decentralized environment where devices communicate and potentially cooperate to perform storage and processing tasks that can be done with or without coordination with centralized cloud applications. As such,
fog computing is a well generalized computing paradigm to be applied in IoT applications [5].

Practical deployment of fog computing needs attention to a number of different aspects such as system design, application design, software implementation, security, computing resource management and networking. The current literature does not cover a comprehensive review of all these aspects. The inter-related nature of these various system dimensions needs an integrated system view identifying the functional components and their interfaces in various layers of the system. Such an integrated view is the main thrust of this paper towards which current state-of-the-art literature has been comparatively reviewed and current trends and future research directions are identified. This paper, however, does not cover the underlying algorithms and enabling technologies in details. Due to their wide variety, they need to be covered in separate surveys in further detail.

A considerable number of surveys have already been published in the general field including [6-8]. In particular, recently, there has been a number of survey papers addressing various aspects of fog computing paradigm.

III. PROPOSED SYSTEM

Smart applications require a rapid response and massive data processing in the sense of the Internet of things (IoT). To meet the two requirements simultaneously, multi-level data processing is essential as illustrated in figure 3. Rim computing resources may include time-sensitive, data aggregation and filtering processes in first order. The more efficient resource may then be central to higher-order processes.

The mechanism proposed is to protect information through creativity in hostile distraction. We screen access to cloud information and identify patterns of strange access to information. In the event of alleged unauthorized access and verified use of challenge queries, we send a breakdown by returning numerous bait details to the attacker. This avoids the misuse of the real knowledge of the consumer.

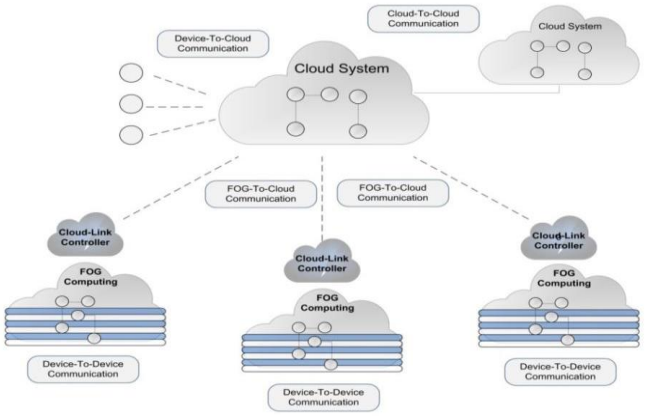

Figure 3. Proposes Architecture

And during the cloud download era, this is upgraded. Distraction data may be generated on interest, for instance, lure papers, nectar records, nectar pots, and various false data as a method to detect unapproved data access and to poison ex filtrated information from cheats. Serving imitations can hop and confuse an intruder if they do not have helpful, ex-filtered data. In order to protect consumer data in the cloud, this new

innovation can be coordinated with customer innovation profiling. Anywhere irregular cloud access is observed, distraction information can be returned and transferred to the Cloud in order to appear fully real and common.

Fog Computing (Fog) is a network architecture that uses close end user-end devices to build up a range of processing, control, configuration, measurement, and management capabilities utilizing storage, communication, and computing resources. Researchers from different backgrounds have approached it since its inception. Consequently, a general consensus on its significance and definition does not exist. Some regard fog computing as an extension to edge computing or as interchangeable with it; otherwise, it is seen as an extension to cloud computing.

IV. RESULTS AND DISCUSSION

A number of cloud-based services are suggested by the way a user can connect to the Internet and storage of data, files, and media in a remote server. A specific issue is the guarantees for protecting user data in a way that guarantees that the user only has access to these data, and no one else does. The topic of the protection of classified information continues to be one of the main security issues that most people do not like.

Many recommendations were made to protect remote cloud data using standard access controls and encryption. Many of the traditional methods, for a number of reasons, are fair to say, have been shown to fail from time to time, including insider attacks, malfunctioning services, unreliable implementation, buggy code, and an innovative structure of efficient and advanced attacks that are not foreseen by security operators [8]. Based on the continued occurrence of incidents and on the knowledge lost there is no way of recovering a trustworthy cloud computing environment. You must brace yourself for such incidents.

The fundamental principle is that if we lower the value of the robbed information to the thief, we can reduce harm to the stolen data. This can be achieved by a "preventive" assault on misinformation. With two additional security features, we propose that stable cloud services can be introduced.

4.1. User Behavior Profiling

Access to information from a user in the cloud is required to represent a standard means of access. User profiling is a well proven technology to model the way a user accesses, where, and how much information a user accesses in the cloud. The actions of such 'average users' can be constantly tested to see if the users' information is irregular. This behavioural safety approach is widely used in cases of fraud. Naturally, such profiles will include volumetric detail, how many records and how many times. Simple user-specific characteristics can be used to detect irregular cloud access based partially on transmitted data scale and scope [9].

4.2. Decoys

Decoy information, including decoys, honeypots and other flawed information, may be created on request to detect unauthorized information and 'poison' the ex-filtered information of the thief. Decoys help to trick and confuse an opponent into thinking that they have valuable knowledge if they do not. The technology can also be used to protect user information in the cloud using user behavior. When an abnormal cloud service access is noted, decoy information can be returned by the Cloud, and provided to the fullest degree possible.

The true user, who is the owner of the information, would readily identify when decoy information is being returned by the Cloud, and hence could alter the Cloud's responses through a variety of means, such as challenge questions, to inform the Cloud security system that it has inaccurately detected an unauthorized access. In the case where the access is correctly identified as an unauthorized access, the Cloud security system would deliver unbounded amounts of bogus information to the adversary, thus securing the user's true data from unauthorized disclosure. The decoys, then, serve two purposes: (1) validating whether data access is authorized when abnormal information access is detected, and (2) confusing the attacker with bogus information. We posit that the combination of these two security features will provide unprecedented levels of security for the Cloud. No current Cloud security mechanism is available that provides this level of security.

V. CONCLUSION

We propose a new approach in this article in the cloud to safeguard personal and corporate data. We propose to track data access habits by profiling user behavior to determine whether or not a malicious insider accesses documents inappropriately in a cloud service. In addition to real user info, decoy documents stored in the cloud are often used as sensors to identify unlawful access. Once unauthorized access or exposure to information has been suspected and subsequently checked for challenges for example, we flood the malicious insider with false information to dilute real user data. Such preventive attacks that rely on disinformation technology, could provide unprecedented levels of security in the Cloud and in social networks.

VI. FUTURE ENHANCEMENT

Concentrating on the future potential of the evolving age of fog, this survey presented nearly immediate use cases that tell us a few short directions in research and distributed versatility application work in the QoS of fog computing frameworks. Fog computing with some dependence can be

classified into computers, communication and stockpiling with existing main technologies. The use of existing main technologies could make Fog networking more intelligent. Together SDN and NFV will improve the scalability of the network as well as the reduction of the cost of live VM migrations.

VII. REFERENCES

[1] S. Yi, C. Li, and Q. Li, ``A survey of fog computing: Concepts, applications and issues," in *Proc. Workshop Mobile Big Data*, New York, NY, USA, 2015, pp. 37_42.

[2] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, ``Fog computing and its role in the Internet of Things," in *Proc. 1st Ed. MCC Workshop Mobile*
Cloud Comput., New York, NY, USA, 2012, pp. 13_16.

[3] S. Yangui, P. Ravindran, O. Bibani, R. H. Glitho, N. Ben Hadj-Alouane, M. J. Morrow, and P. A. Polakos, ``A platform as-a-service for hybrid cloud/fog environments," in *Proc. IEEE Int. Symp. Local Metrop. Area Netw. (LANMAN)*, Jun. 2016, pp. 1_7.

[4] M. Aazam and E.-N. Huh, ``Dynamic resource provisioning through fog micro datacenter," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2015, pp. 105_110.

[5] O. Salman, I. Elhajj, A. Kayssi, and A. Chehab, ``Edge computing enabling the Internet of Things," in *Proc. IEEE 2ndWorld Forum Internet Things (WF-IoT)*, Dec. 2015, pp. 603_608.

[6] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, ``A survey of mobile cloud computing: Architecture, applications, and approaches," *Wireless Commun. Mobile Comput.*, vol. 13, no. 18, pp. 1587_1611, Dec. 2013.

[7] J.-M. Kang, H. Bannazadeh, H. Rahimi, T. Lin, M. Faraji, and A. Leon-Garcia, ``Software-de_ned infrastructure and the future central of_ce," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, Jun. 2013, pp. 225_229.

[8] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, ``Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637_646, Oct. 2016.

[9] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, ``Fog computing: A platform for Internet of Things and analytics," in *Big Data Internet Things: A Roadmap for Smart Environments*. Cham, Switzerland: Springer, 2014,
pp. 169_186.

[10] S. Yi, Z. Qin, and Q. Li, ``Security and privacy issues of fog computing: A survey," in *Proc. Int. Conf. Wireless Algorithms, Syst. Appl.*, 2015, pp. 685_695.

[11] P. Hu, S. Dhelim, H. Ning, and T. Qiu, ``Survey on fog computing: Architecture, key technologies, applications and open issues," *J. Netw. Comput. Appl.*, vol. 98, pp. 27_42, Nov. 2017.

[12] A.Vahid Dastjerdi, H. Gupta, R. N. Calheiros, S. K. Ghosh, and R. Buyya, ``Fog computing: Principles, architectures, and applications," 2016,
arXiv:1601.02752. [Online]. Available: http://arxiv.org/abs/1601.02752

[13] A. V. Dastjerdi and R. Buyya, ``Fog computing: Helping the Internet of Things realize its potential," Computer, vol. 49, no. 8, pp. 112_116,
Aug. 2016.

[14] C. C. Byers, ``Architectural imperatives for fog computing: Use cases, requirements, and architectural techniques for fog-enabled IoT networks,"
IEEE Commun. Mag., vol. 55, no. 8, pp. 14_20, Aug. 2017.

[15] R. Mahmud, R. Kotagiri, and R. Buyya, ``Fog computing: A taxonomy, survey and future directions," in Internet of Everything. Singapore: Springer, 2018, pp. 103_130.

[16] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, ``A comprehensive survey on fog computing: State-of-theart and research challenges," IEEE Commun. Surveys Tuts., vol. 20, no. 1,
pp. 416_464, 1st Quart., 2018.

[17] R. Kumar Naha, S. Garg, and A. Chan, ``Fog computing architecture: Survey and challenges," 2018, arXiv:1811.09047. [Online]. Available:
http://arxiv.org/abs/1811.09047

[18] A. Yousefpour, C. Fung, T. Nguyen, K. Kadiyala, F. Jalali, A. Niakanlahiji, J. Kong, and J. P. Jue, ``All one needs to know about fog computing and related edge computing paradigms: A complete
survey," J. Syst. Archit., vol. 98, pp. 289_330, Sep. 2019.

[19] H. Hejazi, H. Rajab, T. Cinkler, and L. Lengyel, ``Survey of platforms for massive IoT," in Proc. IEEE Int. Conf. Future IoT Technol. (Future IoT), Jan. 2018, pp. 1_8.

[20] M. Eder, ``Hypervisor-vs. container-based virtualization," in Proc. Future Internet (FI) Innov. Internet Technol. Mobile Commun. (IITM), vol. 1, 2016, pp. 11_17.