RESEARCH ARTICLE OPEN ACCESS

From Cloud to Fog Computing: A Review and a Conceptual Live VM Migration Framework

M. Mohamed Faisal*, V. Priya**

*(Asst Professor CSE, Sembodai Rukmani Varatharajan Engineering College, and Sembodai
Email: faisalit85@gmail.com)

** (PG Scholar CSE, Sembodai Rukmani Varatharajan Engineering College, and Sembodai
Email: v995328@gmail.com)

--************************----------------------------------

Abstract:

Fog computing, an addition of cloud computing services to the edge of the network to decrease latency and set of connections congestion, is a relatively recent research trend. Although both cloud and fog offer like resources and services, the latter is characterized by low latency with a wider spread and geographically distributed nodes to support mobility and real-time interaction. In this paper, we describe the fog computing architecture and analysis its different services and applications. We then discuss security and privacy issues in fog computing, focusing on service and resource availability. Virtualization is a vital technology in both fog and cloud computing that enables Virtual Machines (VMs) to coexist in a physical server (host) to share resources. These VMs could be subject to malicious attacks or the physical server hosting it possibly will experience system failure, both of which result in unavailability of services and resources. Therefore, a conceptual smart pre-copy live migration approach is presented for VM migration, which estimates the downtime after each iteration to decide whether to proceed to the stop-and-copy stage during a system failure or an attack on a fog computing node. This will minimize both the downtime and the migration time to assurance resource and service availability to the end users of fog computing. Lastly, future research directions are outlined.

Keywords **— VM migration, Cloud Computing, Fog Computing, Virtualization.**

--************************----------------------------------

I. INTRODUCTION

Cloud computing can be an well-organized choice to owning and maintaining computer resources and applications for many organizations, particularly small- and medium-sized organizations, due to the pay-as-you-go model and other characteristics (e.g., on-demand, self-service, resource pooling and rapid elasticity) [1]. The continual attention in cloud computing has also resulted in other emerging cloud paradigms, such as fog computing. In fog computing, cloud flexible resources are extended to the edge of the network, such as portable devices, smart objects, wireless sensors and other Internet of Things (IoT) devices to decrease latency and network congestion. IoT devices use interconnected technologies similar to Radio Frequency Identify (RFID) and Wireless Sensor and Actor Networks (WSAN) to exchange information over the Internet, and are more integrated in our daily life [2]. Smart-home, smart-city and smart-grid are examples of IoT applications, where sets of sensors are used to find information to improve the quality of life and quality of experiences. IoT is characterized by broadly distributed objects known as “things” with restricted storage and processing capacity to guarantee efficiency, reliability and privacy [3]. However, its applications require geo-distribution, mobility support, location-awareness and low latency [4] to efficiently gather and process data from IoT devices. This information is then used to perform detection and prediction for optimization and sensible decision-making process.

Cloud and fog computing share overlapping features, but fog computing has extra attributes such as location awareness, edge deployment and a large number of geographically distributed nodes in order to recommend a mobile, low latency and real-time interaction [3]. The deployment of together cloud and fog computing is primarily driven by virtualization technology, which introduces a software abstraction between the computer hardware and the operating system (OS) and application running on the hardware [6]. This abstraction layer is also well-known as a Virtual Machine Monitor (VMM) or hypervisor. The VMM acts as a controller of hardware resources and enables multi-tenancy by allowing multiple OS to co-exist on the similar physical hardware and share resources. Despite the benefits afforded by such architecture, cloud services are liable to a range of security and reliability risks. Concerns about attacks or risks disturbing availability of cloud resources are identified in the literature as one of the factors hindering the general adoption of cloud computing [93].

Therefore, live migration of virtual machines (VM) has been planned to mitigate malicious attacks, infrastructural and component failures. Live migration involve a active shift of a VM from one physical machine to another that is transparent to the guest OS, the application consecutively on the OS, and remote users of the VM [6]. Two prime techniques are pre-copy live migration and post-copy live migration [7-8] [10]. The former involves the transfer of memory contents of the VM from a source to a target through several iterations earlier to the VM is restarted; even as the final only sends the virtual central processing unit (vCPU) and the device state to the target at an initial stage [9]. Subsequent pages are fetched on require where the VM is running on the target host. The key performance metrics in VM migration are downtime and complete migration time [10].
This paper presents a exhaustive appraisal of fog computing, its architecture and applications. in addition, we in attendance the security, privacy and resource availability challenges and suggest a novel neat pre-copy VM live migration conceptual framework to cater for malicious attacks stoppage of substantial servers which end result in unavailability of services and resources.

2. LITERATURE REVIEW

2.1Fog Computing Security: A Review Of Current Applications And Security Solutions

Saad Khan*†, Simon Parkinson† and Yongrui Qin discussing with fog computing is a new model that extends the Cloud stage model by providing computing resources on the edges of a network. It can be described as a cloud-like platform having similar data, computation, storage and application services, but is basically different in that it is decentralized. As well, Fog systems are skilled of processing large amounts of data locally, operate on-premise, are fully portable, and can be installed on heterogeneous hardware.

These features make the Fog platform highly proper for time and location-sensitive applications. For example, Internet of Things (IoT) devices are required to rapidly process a large amount of data. This broad range of functionality determined applications intensifies many security issues regarding data, virtualization, segregation, network, malware and monitoring. This paper surveys existing literature on Fog computing applications to identify prevalent security gaps.

Related technologies like Edge computing, Cloudlets and Micro-data centers have also been integrated to offer a holistic review process. The majority of Fog applications are provoked by the desire for functionality and end-user requirements, while the security aspects are often unnoticed or considered as an afterthought. This paper also determine the impact of those security issues and possible solutions, providing future security-relevant directions to those dependable for designing, developing, and maintaining Fog systems.

Fog computing is a decentralized computing architecture whereby data is processed and stored sandwiched between the source of reason and a cloud infrastructure. This results in the minimization of data transmission overheads, and subsequently, improves the performance of computing in Cloud platforms by reducing the necessity to process and store large volumes of superfluous data. The Fog computing example is largely motivated by a continuous enlarge in Internet of Things (IoT) devices, where an ever increasing amount of data is generated from an ever-expanding array of devices.

IoT devices provide wealthy functionality, such as connectivity, and the development of new functionality is frequently data motivated. These devices need computing resources to process the acquired data; however, quick decision processes are also required to maintain a high-level of functionality. This can here scalability and reliability issues when utilizing a standard client-server architecture, where data is sensed by the client and processed by the server. If a server was to turn into overloaded in usual client-server architecture, then many policy could be rendered unusable. The Fog paradigm aims to give a scalable decentralised solution for this issue. This is achieved by creating a new hierarchically spread and narrow platform between the Cloud system and end-user devices [2], as shown in Fig. 1. This platform is able of filtering, aggregating, processing, analysing and transmitting data, and will outcome in saving time and communication resources. This new paradigm is named *Fog computing*, firstly and properly introduced by Cisco [3].

Cloud computing provides many benefits to individuals and organizations during offering highly available and efficient computing resources with an reasonable price [4]. Many cloud services are available in current commercial solutions, but they are not proper for latency, portability and location-sensitive applications, such as IoT, Wearable computing, elegant Grids, Connected Vehicles [5] and Software-Defined-Networks [6]. Latency depends on the rapidity of Internet connection, resource contention among guest virtual machines (VM) and has been shown to raise with distance [7]. Furthermore, such applications generate great volumes of varied data in a high velocity, and by the time data reaches a cloud system for analysis, the possibility to inform the IoT device to get reactive action may be left. For example, consider IoT devices in the medical domain somewhere the latency of acting on the sensed data could be life-critical.

Cisco pioneered the release of the Fog computing model that extends and brings the Cloud platform earlier to end-user's device to establish aforementioned issues.

2.2 Review Distributed Denial Of Service (Ddos) Resilience In Cloud: Review And Conceptual Cloud Ddos Mitigation Framework

Kim-Kwang Raymond Choo , Mqhele Dlodla discussing with in spite of the increasing status of cloud services, ensuring the security and availability of data, resources and services remains an continuing research challenge. Distributed denial of service(DDoS) attacks are not a new threat, but stay a major security challenge and are a topic of continuing research interest. explanatory DDoS attack in cloud presents a new measurement to solutions proffered in usual computing due to its architecture and features. This paper reviews 96 publications on DDoS attack and protection approaches in cloud computing published among January 2009 and December 2015, and discusses obtainable research trends. A taxonomy and a conceptual cloud DDoS mitigation framework based on modify point detection are presented. Upcoming research directions are also outlined.

Cloud computing has turn into a suitable way of accessing services, resources and applications over the internet. This model has shifted the center of industries and organizations away from the deployment and day-to-day running of their IT facilities by providing an on-demand, self-service, and pay-as-you go business representation. Cloud computing has continued to raise in popularity in current times. The National Institute of Standard and Technology (NIST) defines the essential characteristics of cloud computing as on-demand self-service, resource pooling, rapid flexibility and measured service (Mell and Grance, 2011). The service model can be mostly categorized into Software-as-a-service (SaaS), Platform-as-a-Service

(PaaS) and Infrastructure-as-a-Service (IaaS), and it can be deployed as either a private, public, community or hybrid cloud (Tsai et al., 2010). While cloud computing provides a variety of benefits to users, there are also underlying security and confidentiality risks (Khorshed et al., 2012, Christ of et al., 2009, Gonzalez et. For example, multi-tenancy, resource pooling and share capability features can be exploited by cybercriminals and somebody with a malicious intent. This is to the detriment of both the cloud users and providers to exhaust resources which result in denial of services.

In the present Internet-connected society, there is an expectation with the aim of cloud and other Internet services are forever available and any downtime can result in user disappointment. For example, telecommunication industries in some countries need cloud providers to assemble the five 9's availability requirements (Hormati et al., 2014) .Unavailability in cloud can be a result of a number of factors, such as stoppage of cloud infrastructural module or software application and distributed denial of service (DDoS) attacks directed towards the cloud system. For example, cybercriminal groups such as 'Vickingdom2015' had supposedly brought down cloud services (SC Magazine, 2015), resulting in economic loss to both cloud users and providers.

In this paper, we survey general DDoS attacks targeting cloud computing, and categorizes such attacks into application-bug level and infrastructural level attacks. We converse the various tools that could be used to ways or facilitate DDoS attacks, as well as reviewing improvement strategies (e.g. how are DDoS mitigation strategies for cloud computing different from those designed for usual computing).

3. SYSTEM ANALYSIS

System analysis is the generally analysis of the system before implementation and for arriving at a exact solution. watchful analysis of a system before implementation prevents post implementation problems that force arise due to bad study of the problem statement.

Thus the requirement for systems analysis is justified. Analysis is the first essential step, detailed study of the various operations performed by a system and their relationships inside and outside of the system. Analysis is defining the boundaries of the system that will be followed by design and implementation.

3.1 EXISTING SYSTEM

Cloud and fog computing distribute overlapping features, but fog computing has additional attributes such as location alertness, edge deployment and a huge number of geographically distributed nodes in order to offer a mobile, low latency and real-time communication The deployment of both cloud and fog computing is primarily driven by virtualization technology, which introduces a software abstraction between the computer hardware and the operating system (OS) and application running on the hardware. This abstraction layer is also well-known as a Virtual Machine Monitor (VMM) or hypervisor. The VMM acts as a controller of hardware resources and enables multi-tenancy by allowing various OS to co-exist on the same physical hardware and distribute resources. Despite the benefits afforded by such architecture, cloud services are disposed to a range of security and reliability risks. Concerns about attacks or risks affecting availability of cloud resources are identified in the writing as one of the factors hindering the general acceptance of cloud computing

3.1.1 DISADVANTAGE

Low latency with a wider rais and geographically distributed nodes to support mobility and real-time interaction.

3.2 PROPOSED SYSTEM

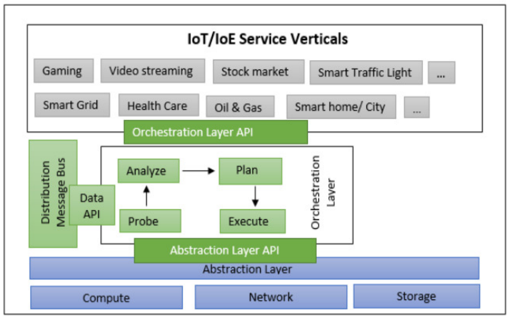
In this paper, we explain the fog computing architecture and evaluation its different services and applications. We then discuss security and privacy issues in fog computing, focusing on service and resource ease of use Virtualization is a vital technology in together fog and cloud computing that enables Virtual Machines (VMs) to coexist in a physical server (host) to distribute resources. These

VMs could be subject to malicious attacks or the physical server hosting it could knowledge system failure, together of which result in unavailability of services and resources. Therefore, a conceptual smart pre-copy live migration approach is presented for VM migration, which estimates the downtime after each iteration to decide whether to proceed to the stop-and-copy stage for the duration of a system failure or an attack on a fog computing node. This will minimize together the downtime and the migration time to assurance resource and service availability to the end users of fog computing. Lastly, upcoming research directions are outlined.

3.2.1 ADVANTAGES

- Heterogeneity geological distribution

4. ARCHITECTURE DIAGRAM



Fog computing has a distributed architecture that targets services and applications with broadly isolated deployments. Different fog computing architectures have been planned in the literature. It described a three-tier architecture where tier 1 is the bottom tier comprising of several terminal nodes (TN) (e.g., smart device and wireless sensor nodes) that send out information to the upper tiers. Tier two is the middle tier (also referred to as the fog computing layer) comprising of extremely intelligent devices, such as routers, switches and gateways.

5. SYSTEM IMPLEMENTATION

Implementation is the phase in the project wherever the theoretical design is turned into a working system. The implementation phase constructs, installs and operates the new system. The most crucial phase in achieving a new successful system is that it will work efficiently and effectively.

There are several activities involved at the same time as implementing a new project.

- End user Training
- End user Education
- Training on the application software

5.1 MODULES

The "**From cloud to fog computing: A review and a conceptual liveVM migration framework**" consists of six major modules.

- Datacenter and Broker Creation
- Virtual Machine Creation
- File Uploading
- Fog Processing to assign
- Access the Cloud

5.2 Module Description

5.2.1 Datacenter and Broker Creation

Datacenter class is a Cloud Resource whose host List are virtualized. It deals with processing of VM queries (i.e., handling of VMs) in its place of processing Cloudlet-related queries. So, still though an Alloc Policy will be instantiated as dealing out of cloudlets are handled by the Cloudlet Scheduler and processing of Virtual Machines are handled by the Vm Allocation Policy. Data centre Broker represents a broker performing on behalf of a user. It hides VM management, as vm formation, sumbission of cloudlets to this VMs and destruction of VMs.

5.2.2 Virtual Machine Creation

Vm represents a VM: it runs inside a Host, distribution host List with other VMs. It processes cloudlets. This processing happens according to a strategy, defined by the Cloudlet Scheduler. Each VM has a owner, which can present cloudlets to the VM to be executed.

6.2.3 File Uploading

In file uploading process, the user choose the file that require to be store in cloud. The selected file is splitted into many packets and shift to cloud.

6.2.4 Fog Processing To Allocate

Fog computing architecture and evaluation its different services and applications. We then discuss protection and isolation issues in fog computing, focusing on service and source availability. Virtualization is a vital technology in together fog and cloud computing that enables Virtual Machines (VMs) to coexist in a physical server (host) to divide resources. In fog process , it decide the data to which virtual machine previous to move to cloud environment.

6. Conclusion

Although early work in fog computing would have been enough to define a fog node as a highly virtualized platform, particulars were absent about the role of edge devices, as well as whether the fog nodes are to be general purpose, or defined in the situation of specific applications, such as eHealth, industrial environment, Smart Cities, etc. The state of the art research identifies a fog node as a mini-cloud, situated at the edge of the network, and close to the IoT policy connected to it.In this paper, we focused on center functionalities of a fog node as fine as in the accompanying opportunities and challenges towards their sensible realization in the near future. We first surveyed the state of the art in technologies for fog computing, paying individual concentration to the contributions that examine the role that edge devices play in the fog node definition. We then summarized and compare the concepts, lessons learned from their implementation, and prove how a conceptual framework is promising towards a unifying fog node definition.

7. Future Enhancement

Security is another big reason companies are revolving to fog computing. Data for applications such as healthcare and point-of-sales connections is very responsive and a primary target for cyber criminals and identity thieves. However, fog computing provides a technique to maintain this type of data under tight guard.Fog systems are designed from the ground up to care for the security of information exchange between IoT devices and the cloud, providing security fit for real-time applications, according to the OpenFog Consortium. Fog systems can also be used to maintain device data securely in-house and gone from vulnerable pubic networks.

References

[1] Osanaiye. O., Choo K-KR., and Dlodlo.M. “Distributed Denial of Service (DDoS) Resilience in Cloud: Review and Conceptual Cloud DDoS Mitigation Framework,” Journal of Network and Computer Applications, vol. 67, pp. 147- 165, 2016.

[2] Díaz M, Martín C, Rubio B. State-of-the-art, challenges, and open issues in the integration of Internet of Things and Cloud Computing. Journal of Network and Computer Applications, 2016 [In Press]

[3] Botta A, de Donato W. Persico V. Pescapé A. Integration of cloud computing and Internet of things: a survey. FuturGener Comp Syst 2016; 56:684-700.

[4] Yi S, Qin Z, Li Q. Security and privacy issues of fog computing: A survey. In: Proceedings of 10th International Conference on Wireless Algorithms, Systems, and Applications, (WASA 2015), Qufu, China; 2015. p. 685-695.

[5] Aazam M, Huh E.-N. Fog computing and smart gateway based communication for Cloud of Things. In: Proceedings of IEEE International Conference on Future Internet of Things and Cloud (FiCloud), Barcelona, Spain; 2014. p. 464–470.

[6] Medina V, García JM. A survey of migration mechanisms of virtual machines. ACM ComputSurv (CSUR) 2014; 46(3):30: 1-33.

[7] Shribman A, Hudzia B. Pre-Copy and post-copy VM live migration for memory intensive applications. In: Series of Lecture Notes in Computer Science in Parallel Processing Workshop (Euro-Par); 2012. p. 539-547.

[8] Deshpande U, You Y, Chan D, Bila N, Gopalan K. Fast server deprovisioning through scatter-gather live migration of virtual machines. In: Proceedings of 7th IEEE International Conference on Cloud Computing (CLOUD), Anchorage, Alaska; 2014. p. 376-383.

[9] Jo C, Gustafsson E, Son J, Egger B. Efficient live migration of virtual machines using shared storage. In: Proceeding of the 9th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environment, Houston, United State; 2013. p. 41-50

[10] Mishra M, Das A, Kulkarni P, Sahoo A. Dynamic resource management using virtual

machine migrations. IEEE Commun Mag 2012; 50(9):34-40.

[11] Yi S, Li C, Li Q. A survey of fog computing: concepts, applications and issues. In: Proceedings of the 2015 ACM Workshop on Mobile Big Data, Hangzhou, China; 2015. p. 37-42.

[12] Bonomi F, Milito R, Natarajan P, Zhu J. Fog computing: A platform for Internet of Things and analytics. In: The Series Studies in Computational Intelligence, Big Data and Internet of Things: A Roadmap for Smart Environments; 2014. p. 169-186.