2581-4575

International Journal For Recent Developments in Science & Technology

Crossref

A Peer Reviewed Research Journal

FOG COMPUTING FOR SECURE AND SUSTAINABLE LOAD BALANCING OF EDGE DATA CENTERS

K. VENKATA SRINIVAS[1], B.GOPI KRISHNA[2]

[1] PG Student, Eswar College of Engineering, Narasaraopet

[2] Asst.Professor, Eswar College of Engineering, Narasaraopet

Abstract: Fog computing is a recent research trend to bring cloud computing services to network edges. EDCs are deployed to decrease the latency and network congestion by processing data streams and user requests in near real time. EDC deployment is distributed in nature and positioned between cloud data centers and data sources. Load balancing is the process of redistributing the work load among EDCs to improve both resource utilization and job response time. Load balancing also avoids a situation where some EDCs are heavily loaded while others are in idle state or doing little data processing. In such scenarios, load balancing between the EDCs plays a vital role for user response and real-time event detection. As the EDCs are deployed in an unattended environment, secure authentication of EDCs is an important issue to address before performing load balancing. This article proposes a novel load balancing technique to authenticate the EDCs and find less loaded EDCs for task allocation. The proposed load balancing technique is more efficient than other existing approaches in finding less loaded EDCs for task allocation. The proposed approach not only improves efficiency of load balancing; it also strengthens the security by authenticating the destination EDCs.

1. INTRODUCTION

An overlapping of the features of cloud along with additional attributes, such as location awareness and EDC deployment, is referred to as fog computing. When distributed geographically in large numbers ,EDC's can provide mobile, low latency data transparency to achieve real-time requests and responses[12].Asapopular choice in providing scalable computation, cloud computing can process large amounts of data (referred as big data), provide storage and provision resources based on the user requirements. Fog computing proposes the migration of cloud resources over to EDCs which are then deployed across the network [21]. The fog computing has various proposed architecture that link it with the edge deployment. A block diagram of the three architectural layers of fog computing is portrayed in Fig. 1. The model begins with the bottom layer compromising of various terminal devices, such as wireless sensors and smart devices, that are responsible for the transmission of data onto the upper layers. The second layer of the model comprises mainly of highly intelligent devices, such as the routers, switches and gateways that aid the network. Some

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

architecture models are known to divide the middle layer, Edge Layer, into its two components; the edge device and the edge datacenter, however in a fog computing architecture these two component layers are combined into as ledge layer. The top mostlayer(alsothethirdlayer)comprisesofseveralhigh-endservers,knownasfogservers,andactsasaclouddatacenter.Thesecloud datacenters, when deployed, also contain user response facilities and occupy the topmost layer of the fog architecture. The fog computing is defined as a combination of the above-statedthree layers as portrayed in Fig. 2 along with its comprehensivearchitectureandvariousmodules.As computing environments achieve great advancements, theEDCservice'savailabilityinfogcomputing hasalsoimprovedrais-ing a lot of attention towards the load balancing problem facedby EDCs. Various research models have been proposed in orderto solve the load balancing problem, however they fail to adequatelyaddresstheconcernsregardingEDCauthentication.Giventhat EDC deployment is usually in remote unattended scenarios,authenticationisanimportantstepbeforeanyloadbalancingtakesplace.Inaddition,asnetworkstructureforanEDCdeploymentisdistributed,theloadbalancingalsoworksinadistributedscenarioand is classified into dynamic load balancing and static load balancing[1].Inthestaticloadbalancingtechnique, theperformancefunctionisminimizedbyprovidingasetofteakstothespecificEDCs.Thiscanbeachievedusingeitherdeterministicmeansorprobabilisticmeans. According to the deterministic balancing technique, EDC-I is responsible for allocation of tasks to EDC-J each time it isrequired. However, in a probabilistic balancing technique, the allocation of tasks done by EDC-I to EDC-K is with a probabilityxandsimilarlyforEDC-Liswithaprobabilityy.Amajordrawbackof static load balancing is due to the fact that it does not takeinto account the status of the destination EDC when deciding theloadbalancing.Thedynamicloadbalancingtakesamorereal-timeapproachbyconsideringthecurrentloadoverindividualEDCandaccordingly suggest a destination EDC. This enables the tasks tobe assigned dynamically from an overloaded EDC to an underloadedoridleEDC.Comparedtothestaticapproach,thedynamicapproach is much difficult to implement, however it provides abetter solution towards achieving a sustainable solution to loadbalancing. Given the above benefits, this paper considers the dynamicloadbalancingtechniqueintheproposedsolution

2. Existing system

In static load balancing, load balancing is achieved by providing a set of tasks to specific EDCs so that the performance function is minimized. This load balancing is done with either deterministic or probabilistic means. In a deterministic balancing technique, EDC-I allocates the over loaded tasks to EDC-J all the time. In a probabilistic balancing technique, EDC-I allocates the overloaded tasks to EDC-K with probability x and to EDC-L with probability y. The major drawback of static load balancing is that it

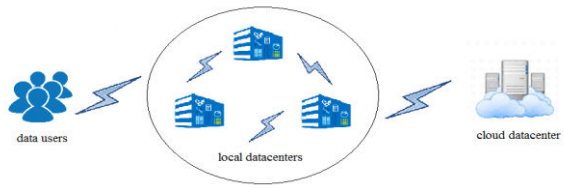
International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

does not consider the status of the destination EDC while making the load balancing decision. In the dynamic load balancing, the current load status of the individual EDCs is considered to decide the destination EDC. As a result, tasks are assigned dynamically from an overloaded EDC to an underloaded EDC for efficient computing.

3. PROPOSED SYSTEM

Based on the current literature survey, there is no such architecture to authenticate the EDC before allocating tasks. Hence, this article proposes a novel architecture to not only authenticate, but also get the load information of the EDCs before sharing the tasks.Based on the fog computing architecture, all the data are stored and processed at the cloud, where EDCs work as the intermediate data centers to reduce the latency of user requests. Cloud is always deployed in the secure environment, so we have considered cloud to initiate the authentication process.This article follows the Breadth First Search (BFS) method to design the proposed load balancing technique. We have used two parameters, m and n, to maintain the load of all the EDCs, where m is the current load and n is the maximum capacity to process the tasks. In order to compute the current load states, we use a parameter p, where p = m/n.

4. ARCHITECTURE



5. IMPLEMENTATION

1. Edge Device

The bottom layer includes several terminal devices such as wireless sensor nodes and smart devices, where these devices transmit data to the upper layers. In the second layer, the fog contains highly intelligent devices, such as routers, switches, and gateways. In some architecture, the middle layer (edge layer) is divided into two parts, edge device and EDC, but most of the fog computing architectures combine these two to form a single layer.

2. Secure Authentication

Based on the fog computing architecture, all the data are stored and processed at the cloud, where EDCs work as the intermediate data centers to reduce the latency of user requests. Cloud is always deployed in the secure environment, so we have considered cloud to initiate the authentication process. Cloud initiates the process to assign initial ID associated with the key and shared key for the individual EDCs during the EDCs' deployment. EDCs use trusted modules (e.g., Trusted Platform Module, TPM) to store the secret information from the cloud and the rekeying process. After initialization of the EDCs, each individual EDC starts to authenticate the EDCs in the region. This helps in the future to avoid malicious EDCs participating in load balancing.

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

3. **Sustainable Load Balancing**

This article follows the Breadth First Search (BFS) method to design the proposed load balancing technique. We have used two parameters, m and n, to maintain the load of all the EDCs, where m is the current load and n is the maximum capacity to process the tasks. In order to compute the current load states, we use a parameter p, where p = m/n. Individual EDCs get load balancing requests from other EDCs to process their tasks. If EDC is overloaded, EDCbroadcasts a control packet by sending requests to other EDCs in the region with its own ID and the received load information. The neighbor EDC checks the received ID and compares it with its own database. In the case of a match, EDC then looks for the load information from the control packets; otherwise, it ignores the control packet to avoid a denial of service attack. While checking the EDC load information, EDC first checks its own load information using a value of p. If p is less than or equal to 0.6, it moves forward to get the available resources (i.e., n – m) to process the invited tasks. If the available resource is higher than the required resource to process the invited task, EDC processes the positive response packet to EDC. Otherwise, EDC becomes silent without any response.

4. **Cloud Data Center**

The third andtopmost layer tends to be the cloud data centercomprising several high-end servers. Cloud datacenters have user response facilities. The main difference between a cloud and a data center is that a cloud is an off-premise form of computing that stores data on the Internet, whereas a data center refers to on-premise hardware that stores data within an organization's local network. While cloud services are outsourced to third-party cloud providers who perform all updates and ongoing maintenance, data centers are typically run by an in-house IT department.

5. **ALGORITHM**

1. **Advanced Encryption Standard (AES)**

The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption. AES, or Advanced Encryption Standards, is a cryptographic cipher that is responsible for a large amount of the information security that you enjoy on a daily basis. Applied by everyone from the NSA to Microsoft to Apple, AES is one of the most important cryptographic algorithms being used in 2018.

2. **Breadth First Search (BFS)**

A breadth first search traversal method, visits all the successors of a

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

visited node before visiting any successor of any of its child nodes. This is a contradiction to depth first traversal method; which visits the successor of a visited node before visiting any of its brothers, i.e., children of the same parent. A depth first traversal method tends to create very long, narrow trees; whereas breadth first traversal method tends to create very wide, short trees. This article follows the Breadth First Search (BFS) method to design the proposed load balancing technique.

6. CONCLUSION

This article proposes a novel secured and sustainable load balancing solution for EDCs in fog computing environment. The proposed load balancing technique is basically divided into two major parts, where the first part focuses on secure authentication of the EDCs in the region by using cloud initiated credentials, followed by a sustainable load balancing architecture by getting load information of the destination EDCs. The proposed solution has been evaluated in two different ways, using both theoretical analysis and experimental evaluation. From the performance evaluation and comparison results, we conclude that the proposed solution is secure and sustainable by getting destination EDC's load during the authentication process. As EDCs are deployed in an open and hostile environment, we propose a security solution to protect against outsider attacks by authenticating the destination EDCs and avoiding malicious ones.

Future work

In the future, we plan to extend our research avenues by proposing lightweight security solutions and improving load balancing performance of EDCs in fog computing environments. In addition to this, we are building a real-time testbed to implement the proposed security and load balancing scheme.

References

[1] O. Osanaiye et al., "From Cloud to Fog Computing: A Review and a Conceptual Live VM Migration Framework," IEEE Access, vol. 5, no.1. 2017, pp. 8284–8300.

[2] L. Tong, Y. Li, and W. Gao, "A Hierarchical Edge Cloud Architecture for Mobile Computing," Proc. IEEE INFOCOM 2016, 2016, pp. 1–9.

[3] M. S. Obaidat and P. Nicopolitidis, Smart Cities and Homes: Key Enabling Technologies, Morgan Kaufmann, 2016. ISBN: 978-0-12-803454-5.

[4] M. S. Obaidat and S. Misra, Principles of Wireless Sensor Networks, Cambridge Univ. Press, 2014. ISBN: 978-0-521- 19247-7

[5] A. Alakeel, "A Guide to Dynamic Load Balancing in Distributed Computer Systems," Int'l. J. Computer Science Info. Security, vol. 10, no. 6, 2010, pp. 153–60.

[6] K-K R. Choo et al., "A Foggy Research Future: Advances and Future Opportunities in Fog Computing Research," Future Generation Computer Systems, vol. 78, no. 2, 2018, pp. 677–79.

[7] M. Jia et al., "Cloudlet Load Balancing in Wireless Metropolitan Area Networks," Proc. IEEE INFOCOM 2016, 2016, pp. 1–9.

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

[8] M. Willebeek-LeMair and A. Reeves, "Strategies for Dynamic Load Balancing on Highly Parallel Computers," IEEE Trans. Parallel Distrib. Systems, vol. 4, no. 9, 1993, pp. 979–93.
[9] Y. Zhang et al., "Joint Bidding and Geographical Load Balancing for Data centers: Is Uncertainty a Blessing or a Curse?" Proc. IEEE INFOCOM 2017, 2017, pp. 1–9.
[10] D. Puthal et al., "Threats to Networking Cloud and Edge Data Centers in the Internet of Things," IEEE Cloud Computing, vol. 3, no. 3, 2016, pp. 64–71.
[11] I. Butun et al., "Cloud-Centric Multi-Level Authentication as a Service for Secure Public Safety Device Networks," IEEE Commun. Mag., vol. 54, no. 4, Apr. 2016, pp. 47–53.
[12] D. He and S. Zeadally, "Authentication Protocol for an Ambient Assisted Living System," IEEE Commun. Mag., vol. 53, no. 1, Jan. 2015, pp. 71–77.
[13] D. Puthal et al., "A Synchronized Shared Key Generation Method for Maintaining End-to-End Security of Big Data Streams," Proc. 50th Hawaii Int'l. Conf. System Sciences, 2017, pp. 6011–20.
[14] D. Puthal et al., "Building Security Perimeters to Protect Network Systems against Cyber Threats," IEEE Consumer Electronics Mag., vol. 6, no. 4, 2017, pp. 71–77.

AUTHORS PROFILE

K. VENKATA SRINIVAS is a student pursuing M.Tech(CSE) in Eswar college Of Engineering, Narasaraopet, Guntur

B. GOPI KRISHNA M.Tech in Computer Science & Engineering. He is currently working as an Asst Professor in Eswar College of Engineering, Narasaraopet, Guntur, India. He is having about 4 years of teaching experience in different Engineering Colleges