Secure and Sustainable Load Balancing ofEdge Data Centers in Fog Computing

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.

CONTINUE

- This article proposes a novel load balancing technique to authenticate the EDCs and fnd 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.
- g

EXISTING SYSTEM

- Fog computing exhibits some of the overlapping features of cloud with additional attributes such as location awareness and edge data center (EDC) deployment. A large number of EDCs are geographically distributed to offer mobile, low-latency data transparency over real-time requests and responses .
- Cloud computing is popular for scalable computation and processing of large amounts of data (referred to as big data). This is also popular for storage and provisioning of resources according to user requirements.

PROPOSED SYSTEM

- This Paper proposes a novel load balancing technique to authenticate the EDCs and fnd 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.
- The proposed approach presents an adaptive EDC authentication technique with the help of a centralized cloud data center. This authentication is initiated by the cloud and then all EDCs authenticate each other by following cloud credentials.

CONTINUE

- The proposed approach brings a sustainable and dynamic load balancing technique by considering the load of the destination EDCs. This load information is shared during the authentication process, so individual EDCs do not need additional communication to get the load information from others.
- Finally, the proposed approach combines both the authentication and load balancing techniques to apply in the EDCs. The proposed approach also evaluates the performance by validating the efficiency and scalability.

HARDWARE REQUIREMENTS

- Processor - Pentium –III
- Speed - 1.1 Ghz
- RAM - 256 MB(min)
- Hard Disk - 20 GB
- Floppy Drive - 1.44 MB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

SOFTWARE REQUIREMENTS

- Operating System : Windows 8
- Front End : Java /DOTNET
- Database : Mysql/HEIDISQL

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.

REFERENCE

[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.

CONTINUE

[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.