Fog Computing Based Recovery Model for Reliable E-Healthcare Services

Humaiz Shaikh*[1], Muhammad Yaqoob Koondhar[2], Ali Raza[3], Zulfikar Ahmed Maher[4], Asadullah Shah[5]

Abstract: **Fog computing is an architecture that extends traditionally centralized cloud computing functions to the edge and close to where data is generated from the Internet of Things (IoT) network, saving the cloud bandwidth and reducing the processing time required. Urgent data generated from Internet of Things (IoT) devices such as data on health intensive care, data on disaster detection or some critical business data need to be processed quickly to obtain real-time notification and then take appropriate action. However, it is necessary to ensure continuity of operation for these systems even in the event of a network failure, which is an issue not yet well addressed in the literature. In this regard, the purpose of this paper is to explore and evaluate the current techniques used in the context of fog computing for failure recovery and to propose a fog based recovery model using a replication technique to ensure the reliability of time-sensitive healthcare systems. The suggested design will be tested using a simulator**

***Keywords*— Fog Computing, Node Failure, Failure Recovery, .Service Reliability, E-healthcare**

INTRODUCTION

Today, a enormous quantity of information is produced, particularly in the presence of Internet of Things (IoT), which is transmitted and handled in a core cloud [1]. Urgent information produced from IoT such as information on health surveillance, information on disaster detection systems needs to be processed quickly to obtain a reply in real time to take the suitable intervention. However, the enormous quantity of information transferred to a cloud make cloud storage inefficient in near real-time processing of emergency information [2]. Fog computing emerges to resolve this problem by evaluating and handling these information at a stage close to the location from which it is produced in a fog server. While this method will not avoid accidents, it will decrease the harm it creates by promptly informing government security officials in the event of a natural disaster detection systems that will save many lives [3]. This study focuses on the weakness of healthcare technologies in their time sensitive to information, which is the primary problem for emergency applications where time is a vital variable in their efficiency.

[1-5]International Islamic University Malaysia,
[2-4]Sindh Agriculture University Tandojam,
[3]University of Sufism and Modern Sciences Bhit Shah
Email: humaiz_shaikh@hotmail.com

IDENTIFIED PROBLEMS IN FOG COMPUTING

Although fog technology is still in its infancy, it is commonly embraced in various fields such as healthcare, vehicle networks, intelligent cities/industries and disaster detection systems [4]. Existing fog-node computing platforms and middle-ware cannot effectively acquire emergency information in the event of fog-node failure that could cause enormous harm [2]. Frequent optimization of present information leadership methods is essential for more efficient and safe emergency structures [5]. However, due to the pressing information produced from edge systems, few trials have been performed to recover from a crash. This research suggests a model of failure recovery that aims to provide urgent data a higher chance of reaching the authority parties in real time even if the fog server fails to deliver the data can save a life.

FOG COMPUTING

Fog computing technology is a three layered design (Cloud-fog-edge) aimed at transferring computing energy near the end user[6]. Although fog technology is still in its infancy, it is commonly embraced in various fields such as healthcare, vehicle networks, intelligent cities/industries, and technologies for disaster detection systems [4]. However, if a fog server fails, few studies have been completed to contract with immediate data generated from fog devices. In this respect, this research will address and extend equivalent research work already being conducted in E-Healthcare services on fog server failure recovery techniques.

Fog Computing in Healthcare

IoT has received the helpfulness of the healthcare community due to the growing amount of medical facilities, sensors and portable phones that are interconnected through the internet. IoT is considered a successful option for the healthcare industry because it can change the diagnosis technique away from hospitals and arrange for customers with the capability to access care remotely, handle their own disease on their own and obtain help through a mobile technology [7]. As a result, the cloud computing effort expands and because the cloud servers get overloaded the network will experience a bigger latency. Recent research efforts have therefore focused on unloading to the edge of the network some of the tasks (e.g. storage or processing tasks) usually performed in the cloud [8]. Fog computing is considered as the finest method to depend on as these applications are susceptible to latency, demonstrate poor reaction time and generate big amount of data. Fog computing contributes significantly to health

applications by serving the elderly through home nursing [9] .

Healthcare Systems Reliability

The cloud computing approach needs secure Internet connectivity at steady elevated speeds with adequate bandwidth and low latency [10].In the event that either the bandwidth is insufficient or any other network failure occurs, cloud can result in increased delays and become a single point of failure that cannot be allowed throughout the healthcare system. In addition, IoT devices ongoing interaction with the cloud improves power usage. Therefore, cloud computing cannot meet IoT applications requirements for real-time data handling because it requires ongoing and efficient relationships with low latency between IoT technologies and healthcare services. While the provision of healthcare services becomes more reliant on on network connections, network defects can disrupt or stop the provision of healthcare services with negative impacts on the quality of lives of individuals, even leading to death [7].

Fog Server Failure

Fog computing offers functions that the cloud computing strategy cannot naturally endorse, including customer mobility assistance, place consciousness, geographic allocation, low latency, and delays. These features are important to deliver delay-sensitive facilities such as healthcare and urgent facilities. System failures have different consequences depending on what data is used for, ranging from minor inconvenience to serious threats to the lives of patients. Accordingly, reliability is one of the most significant criteria to consider, closely interconnected with safety threats resilience [7]. Like the cloud, there is also a failure of fog computing nodes. Like the cloud, there is also a loss of fog computing nodes. Nevertheless, the implications and nature of failure differ from cloud computing. Failures in the cloud or network may influence a hospital as a whole. By comparison, if reduced network structure fail, the effects will impact a narrower region, such as segments of hospitals or single patients. Such minor accidents with regard to re-equipment or re-stuffing are often simpler to manage. Fog computing can also result in architectures with built-in redundancy at the local stage, with multiple fog computing nodes functioning as fault tolerant sets that increase reliability [11][12]. Many IoT applications are going to be critical to assignment or even critical to lives. These applications must proceed to function as anticipated even if they are down or severely overloaded with cloud assets or the network connections required to achieve them. Local fog servers, even if the cloud does not respond, can provide backup service logic. They may not have the cloud's full capacities, but they often have enough fundamental local features to retain critical facilities until they can restore cloud processing. Collection of multiple fog servers can function as fault tolerant sets to support the implementation on the surviving useful fog servers, even if other nodes in the collection do not work [11].

Current Techniques used to deal with Fog Server Failure

A service protection in F2C has been implemented, designed and evaluated, taking into consideration two failure retrieval approaches:

- So called proactive security, wherever security funds are pre-allocated and used in the event of main resource failure.
- Reactive security, where secondary funds are not assigned until a failure happens.

In an attempt to address this research, proactive and reactive protection approaches against product failures are formalized using linear programming. The objective was to provide sufficient computing resources to resist failures of single products. Assuming a cloud fog F2C situation in which only Fog technology failures are feasible. The validation behind this hypothesis is to demonstrate Fog server's weakness and its effect on the efficiency and price of service transmission. An assessment of the outcomes provided indicates that on F2C architectures both proactive and reactive restoration of failure in possible [13].

FAILURE RECOVERY IN FOG COMPUTING

The primary objective of this research paper is to add to enhancing the efficiency of real-time fog computing oriented devices and gain knowledge into the present latency and fault tolerance research work. Regarding the awareness of the moment in such schemes and the restricted study work considering optimizing information dissemination processes in the case of Fog server failure; this study refers to the methodologies of healthcare real-time technologies to suggest additional optimization and suggestions for more accurate growth of real-time technologies [14]. This research explores and evaluates the current techniques used for failure recovery of a fog server in emergency healthcare services due to its time sensitivity. Then, a failure recovery model is proposed based and will be tested using ifogsim simulator.

Failure Recovery Model

The health data from the sensors are connected to a fog node (e.g. wearable device and smartphone) which reads the data frequently and send two copies of those data to the closer to fog servers [15] [16]. The main server and the backup server. Since fog servers can perform complex operations and analysis due to their high computational capabilities, they detect the abnormal sensor values. The terms abnormal is referred to any value that is above or less than pre-defined normal range [7]. Both fog servers process the coming value, if the processed value is identified as abnormal value, the main fog server sends that value to the patient monitoring record in the cloud. When the cloud receives that value, it send an acknowledgment (Ack) message to the backup fog server. Which indicates that the abnormal value reached the cloud. Then, authority parties will get a notification from the cloud for abnormal value, to take the immediate action as

soon as possible. However, in some cases, the main fog servers might not be able to process the sensitive information due to system down or power interruption. So, the backup fog server will send the abnormal value to the cloud if the backup server hasn't got the acknowledgment message within a specific period of time [17].

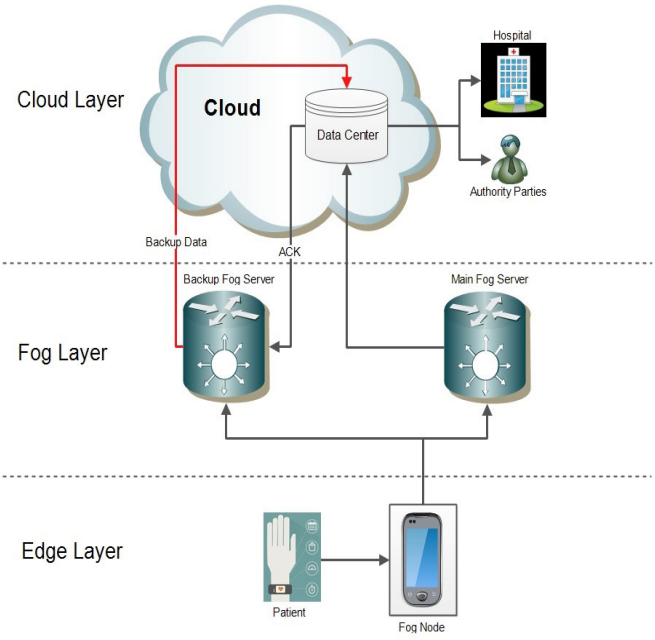

Fig1. Failure Recovery Model for Urgent Data

This Model Consists of 5 Elements:

Fog node: devices aggregating data from several mixed IoT applications such as medical environmental detectors, smartphones and game cameras.

Main Fog Server: fog server is a type of cloud server that collects, stores, processes, and analyzes IoT device information. In addition, the fog server must decide which information should be sent to the cloud, which data type, and when because fog servers have elevated computing capacities that are installed at the bottom of the network such as gateways, home-based low-power pcs, shopping centers, bus terminals, railway stations, and parks.

Backup Fog Server: is like the main server, except that it works as a backup server that can be used when needed.

Cloud: provides continuous storage of data warehouse, conducts big data assessment and other back-end applications. The data store contains a patient record table that is associated with an address table which contains information to source device address (fog node) and the main server address (fog server) and the backup server address.

Authority parties: sectors that are responsible for taking the immediate action when an abnormal value notification occurs.

CONCLUSION

This paper proposes a failure recovery model, dealing with fog server failure particularly. Which mainly aims to save lives in emergency cases, when a single second could make a difference. The proposed model adopts a data duplication technique to recover from a fog server failure on the fog layer, to provide a high chance for critical data to reach the cloud even in the presence of failure. Ifogsim simulator will be used to evaluate the possibility of the proposed model in terms of time delay.

REFERENCES

[1] M. Femminella, M. Pergolesi, and G. Reali, "IoT , Cloud Services , and Big Data : A Comprehensive Pricing Solution," in 2016 Cloudification of the Internet of Things (CIoT), 2016, pp. 1–5.

[2] M. Achouri, A. Alti, M. Derdour, S. Laborie, and P. Roose, "SMART FOG COMPUTING FOR EFFICIENT SITUATIONS MANAGEMENT IN SMART HEALTH ENVIRONMENTS," J. Inf. Commun. Technol., vol. 17, no. 4, pp. 537–567, 2018.

[3] A. Rauniyar, P. Engelstad, B. Feng, and D. Van Thanh, "Crowdsourcing-based Disaster Management Using Fog Computing in Internet of Things Paradigm," in 2016 IEEE 2nd International Conference on Collaboration and Internet Computing, 2016, pp. 490–494.

[4] J. Park and Y. Park, "Fog-based File Sharing for Secure and Efficient File Management in Personal Area Network with Heterogeneous Wearable Devices," J. Commun. Networks, vol. 20, no. 3, pp. 279–290, 2018.

[5] K. Pawar and V. Attar, "A Survey on Data Analytic Platforms for Internet of Things," in 2016 International Conference on Computing, Analytics and Security Trends (CAST), 2016, pp. 605–610.

[6] L. Gao, T. H. Luan, S. Yu, W. Zhou, and B. Liu, "FogRoute: DTN-Based Data Dissemination Model in Fog Computing," in IEEE Internet of Things Journal, 2017, vol. 4, no. 1, pp. 225–235.

[7] F. Andriopoulou, T. Dagiuklas, and T. Orphanoudakis, "Integrating IoT and Fog Computing for Healthcare Service Delivery," in Components and Services for IoT Platforms, 2017, pp. 213–232.

[8] R. Craciunescu, A. Mihovska, and S. Halunga, "Implementation of Fog Computing for Reliable E-Health Applications," 2015, pp. 5–9.

[9] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and A. Polakos, “A Comprehensive Survey on Fog Computing : State- of-the-art and Research Challenges,” in IEEE Communications Surveys & Tutorials, 2017, no. 1.

[10] M. Firdhous, O. Ghazali, and S. Hassan, “Fog Computing : Will it be the Future of Cloud Computing ?,” in Proceedings of the Third International Conference on Informatics & Applications, Kuala Terengganu, Malaysia, 2014, 2014, pp. 8–15.

[11] C. C. Byers and P. Wetterwald, “Fog Computing: Distributing Data and Intelligence for Resiliency and Scale Necessary for IoT,” Advancing Computing as a Science & Profession, no. November 2015, pp. 1–12, Nov-2015.

[12] F. A. Kraemer, A. E. Braten, N. Tamkittikhun, and D. Palma, “Fog Computing in Healthcare — A Review and Discussion,” vol. 5, no. May, pp. 9206–9222, 2017.

[13] V. B. Souza, X. Masip-bruin, E. Marín-tordera, W. Ramírez, and S. Sánchez-lópez, “Proactive vs Reactive Failure Recovery Assessment in Combined Fog-to-Cloud (F2C) Systems,” in 2017 IEEE 22nd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2017.

[14] M. S. A. Md. Muzakkir Hussain and M. M. S. Beg, “Fog Computing in IoT Aided Smart Grid Transition-Requirements, Prospects, Status Quos and Challenges,” Cornell Univ., pp. 1–13, 2018.

[15] Y. Chen, E. Sun, and Y. Zhang, “Joint Optimization of Transmission and Processing Delay in Fog Computing Access Networks,” in 2017 9th International Conference on Advanced Infocomm Technology (ICAIT), 2017, pp. 155–158.

[16] W. Li, Y. Yang, I. Senior, D. Yuan, and I. Member, “Ensuring Cloud data reliability with minimum replication by proactive replica checking,” in IEEE Transactions on Computers (Volume: 65 , Issue: 5 , May 1 2016), 2015, pp. 1–14.

[17] V. STANTCHEV, A. BARNAWI, S. GHULAM, J. SCHUBERT, and G. TAMM, “Sensors & Transducers Smart Items ,Fog and Cloud Computing as Enablers of Servitization in Healthcare,” IFSA Publ. S. L., vol. 185, no. 2, pp. 121–128, 2015