"(c) 2016 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other users, including reprinting/ republishing this material for advertising or promotional purposes, creating new collective works for resale or redistribution to servers or lists, or reuse of any copyrighted components of this work in other works."

Crowdsourcing-based Disaster Management using Fog Computing in Internet of Things Paradigm

Ashish Rauniyar*, Paal Engelstad†, Boning Feng‡, Do Van Thanh§
*†‡§Department of Computer Science, Oslo and Akershus University College of Applied Sciences, Oslo, Norway 0166
*†Department of Informatics, University of Oslo, Oslo, Norway 0316
§Telenor Research and Development, Telenor, Oslo, Norway 1360
Email: (*ashish.rauniyar,†paal.engelstad,‡boning.feng,§thanh-van.do)@hioa.no

***Abstract*—In internet of things (IoT) paradigm, crowdsourcing is the process of obtaining and analyzing information or input to a particular task or project generated by a number of sources such as sensors, mobile devices, vehicles and human. Cloud computing is widely used for the services such as analyzing crowdsourced data and application implementation over the IoT. Nowadays, every country and human are prone to natural and artificial disasters. Early detection about disasters such as earthquakes, fire, storms, and floods can save thousands of people's life and effective preventive measure can be taken for the public safety. All the crowdsourced data which are providing the information of a certain geographic region are analyzed in a cloud platform. But, by the time the crowdsourced data makes its way to the cloud for analysis, the opportunity to act on it might be gone. Moreover, thousands of people's life will be lost. Therefore, fog computing is the new and efficient way to analyze such critical crowdsourced IoT data of disasters. In this paper, in order to detect and take necessary steps for public safety during a disaster, we propose a crowdsourcing-based disaster management using fog computing (CDMFC) model in IoT. Further, we also proposed a data offloading mechanism for our CDMFC model to send disaster-related IoT data to the fog even if a direct link to the fog is not available. Our proposed CDMFC model and its data offloading mechanism can detect real-time disasters and disseminate early information for public safety as compared to the conventional cloud computing based disaster management models.**

I. Introduction

The internet of things (IoT) is the network of physical objects such as sensors, mobile devices, buildings, vehicles which are further embedded with software, electronics and network connectivity which enable these objects to collect and exchange data between them [1][2]. Over the past few years, IoT has gathered a lot of interest from both industry and research community. The business opportunities with IoT is rapidly increasing. It is estimated by the experts that the IoT will consist of almost 50 billion objects by 2020 and the amount of data generated by these objects will be huge [3]. In IoT paradigm, the process of obtaining and analyzing information or input to a particular task or project generated by a number of these objects is termed as crowdsourcing [4]. Cloud computing is widely used for the services such as analyzing crowdsourced data and application implementation over the IoT [5]. As stated, cloud computing makes computing resources such as application development platform, hardware and computer applications available as services over the internet. The services made available through this manner are commonly known as Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) [6]. Using IoT and these services, crowdsourcing combines sensing technologies, analytical models, data management techniques and visualization methods to create solutions to improve the quality of human life and its surrounding environment.

Nowadays, every country and human are prone to natural and artificial disasters. Earthquake, flood, hurricane, typhoon etc. comes under natural disaster and fire, bombings, traffic jam etc. are artificial or man-made disasters. We have already witnessed several of disasters all around the world costing lives of millions of peoples and yet to see more in coming years. Natural and artificial disasters are the sudden events that requires an immediate action by the public safety authorities and government organizations to save the lives of millions of peoples trapped in such situations and provide necessary rehabilitation facilities to them. Developing countries are disproportionately exposed to the risks of natural disasters, and often have limited means to mitigate their effects due to high population density, poor evacuation infrastructure and exposure to severe weather events. IoT technologies cant stop disasters from happening, but can be very useful for disaster preparedness, such as prediction and early warning systems and rescue operation post disasters. In this way, IoT can compensate for a poor infrastructure [7].

The application of integration of crowdsourcing IoT data with cloud computing platform is in many areas. But, due to the limitation of cloud computing platform, they not suitable for real-time events such as disaster and natural calamities management. In cloud computing platform, real-time events with which users directly interact with are badly affected by delay and jitter caused by latency in networks. Take for example, the monitoring of certain earthquake prone geographical region: motion sensors on such locations take measurements and continuously send crowdsourced data to the cloud for analysis. Only after data management and analytics in a cloud platform, we can arrive at a certain conclusion which might cost the lives of millions of people. One of the possible ways to overcome this weakness of cloud computing paradigm is edge computing or fog computing [8]. Instead of sending a vast amount of crowd-sourced IoT data

978-1-5090-4607-2/16 $31.00 © 2016 IEEE
DOI 10.1109/CIC.2016.72

IEEE computer society

TABLE I
CLOUD COMPUTING V/S FOG COMPUTING

Requirement	Cloud Computing	Fog Computing
Latency	High	Low
Delay Jitter	High	Very low
Location of server nodes	Within the Internet	At the edge of the local network
Distance between the client and server	Multiple hops	One hop
Security	Undefined	Can be defined
Attack on data enroute	High probability	Very low probability
Location awareness	No	Yes
Geographical distribution	Centralized	Distributed
Support for Mobility	Limited	Supported

to the cloud, fog computing analyses the most time-sensitive data at the network edge, close to where it is generated. It also acts on crowdsourced IoT data in milliseconds based on pre-defined policy and sends selected data to the cloud for historical analysis and longer-term storage. A comprehensive difference between cloud and fog computing is outlined in Table I [9]. Any device with network connectivity, computing and storage can act as a fog computing node such as routers, switches, embedded servers, industrial controllers and video surveillance cameras.

In this paper, with the aim of taking the advantages of crowdsourcing and fog computing to handle disaster management in an efficient way, we propose a crowdsourcing-based disaster management using fog computing (CDMFC) model in IoT. Further, a data offloading mechanism is proposed for our CDMFC model if a direct link to the fog is not available considering the poor communication infrastructure during the disaster time. Data offloading mechanism in CDMFC model makes sure that disaster-related IoT data is successfully sent to the fog. As compared to the conventional cloud computing based disaster management models, our proposed CDMFC model can detect real-time disasters and disseminate early information for public safety.

The rest of the paper is organized as follows. In Section II, related work and the background is briefly explained. Section III explains the procedural flow and hierarchical layered structure of our proposed CDMFC model. Conclusion and future works in drawn in Section IV.

II. BACKGROUND AND RELATED WORKS

With the advent of cloud computing technologies and crowdsourcing, IoT provides a reliable platform to disseminate information early for the public safety during the disasters and public safety authorities can launch rehabilitation operation for disaster affected areas and peoples. During the one of the major earthquake (magnitude of 7.8 on Richter scale) in Nepal which occurred on 25 April 2015, killed over 8,000 people and more than 21000 were injured [10]. Soon, many people updated the live happening of the earthquake through data, picture and videos on social media platform like Facebook

Fig. 1. Safety check feature from Facebook during Nepal's earthquake [12]

and Twitter etc. The crowdsourced data through social media were really helpful to launch rehabilitation program to reach out to the needy people trapped in the affected region. When such disasters happen, people also need to know their loved ones are safe. Thus, Facebook came up with a new and innovative feature called 'Safety Check' [11]. The 'Safety Check' feature can quickly determine whether people in the affected geographical area are safe during such natural or man-made disasters. When Safety Check feature is activated, it locates Facebook users near a disaster site from where they used the internet or through the city they listed on their profile. Facebook users are then asked to confirm whether they are safe or they are in disaster affected areas. Those Facebook users who choose option "safe", generate a notification message to their family members, followers, and friends, who in turn can track how many of their friends/family members/followers were affected. This 'Safety Check' feature is based on the crowdsourcing model to disseminate the information as soon as possible so that effective rescue can be planned accordingly. A 'Safety Check' feature from Facebook launched during the Nepal earthquake is shown in Fig. 1.

In our previous work [13], we demonstrated an earthquake

detection system with the integration of wireless network to transmit the data and video of the earthquake location as a crowdsourcing IoT data model for disaster management. The model was based on sensing and sending earthquake sensor data and video of the earthquake-prone region continuously to the server or cloud for the analysis. If a shake is detected by the sensor then an alert is sent to the public safety officer on his/her cell phone to take necessary step for saving millions of life during such disaster. However, a time delay was there in our model and our earthquake detection system could be more efficient if we would have used fog computing for this critical event.

A trustworthy sensing for crowd management (TSCM) model for the front end access to the IoT has been proposed in [14]. Sensing data by the mobile users were crowdsourced to the cloud platform for public safety analysis. An auction mechanism was also performed to select the mobile devices for the particular sensing task. The mobile devices were provided incentives for providing the credible sensing data. TSCM model utilized the sensing as a service scheme. Combining IoT with crowdsourcing in a common platform for managing emergency situations has been analyzed in [15]. The authors utilized the IoT data and more contextual information provided by the people to enhance and subsequently manage the emergency situations. Reference [16] argued that, during the disaster period, vast deployment of IoT-enabled devices could bring benefits in terms of data network resilience. While the conventional communication service is out of service during a disaster, the IoT devices could enable emergency micro-message delivery communication service through data prioritization schemes. A 5W (What, Where, When, Who and Why) model based on social media big data has been proposed in [17] for managing urban emergency events. In 5W model, the users of social media have been set as the target of crowdsourcing. However, most of these schemes focused on cloud computing platform which has its own disadvantage in terms of delay. Also, an efficient method to deliver time-critical sensing data successfully to the central authority or cloud during disaster situation considering poor communication infrastructure has not been studied so far in the literature. This motivated us to propose CDMFC model and data offloading mechanism for disaster management.

III. Proposed Model

In this section, our crowdsourcing based disaster management using fog computing model in IoT which we call it as CDMFC model will be explained along with data offloading mechanism.

The procedural flow and hierarchical layered structure of our proposed CDMFC model are shown in Fig. 2 and Fig. 3 respectively. CDMFC model consists of four layers namely sensing, crowdsourcing, CDMFC and cloud computing layer.

A. Sensing Layer

This layer is dedicated to sensing of a different event such as fire, earthquake, flood, other natural and artificial disasters and many other IoT applications through sensors, mobile phones, laptops, tablet etc. A data related to events is also generated by humans through mobile phones and tablets which can be viewed as social sensors [14]. It is to be noted that huge amount of data will be generated due to sensing related to different IoT applications. Not, all these sensed data are related to disasters and emergency events. The sensing layers only sense different event and generate sensing data irrespective of the type of events.

B. Crowdsourcing Layer

This layer is dedicated to crowdsourcing all the sensing data generated from the sensing layer. In most of the proposed work, all these crowdsourced data are directly sent to the cloud for further analysis where data mining and other techniques are applied on data to make a knowledge base. To make a knowledge base and arrive at a final conclusion in cloud computing platform takes time. However, if billions of IoT devices are connected with each other, huge amount of IoT data will be crowdsourced to the cloud and this will lead to taking a lot of time to prepare and rescue operation for public safety during disaster and emergency events which will eventually cost the lives of millions of people. In our proposed CDMFC model, the disaster-related and emergency events are sent directly to the CDMFC layer for effective disaster management for public safety. The quick question arises here is how crowdsourcing layer is going to send the only disaster related emergency events data to CDMFC layer. CDMFC model adopts filtering technique based on emergency and disaster-related keywords generated by the IoT applications and humans through different mobile phones and tablets and sensors deployed in disaster-prone region or location.

Further, it should be noted that, during disaster time, a direct link to the fog/CDMFC layer may not be available due to poor communication infrastructure. The sensors may not be able to send crowdsourced data. In such situation, our CDMFC model uses data offloading mechanism. CDMFC model first checks whether a direct link to Fog/CDMFC layer is available or not. If the link is available then the crowdsourced disaster-related IoT data is directly sent to the fog/CDMFC layer. If the direct link is not available, CDMFC layer offloads the data to the nearest smart IoT objects such as smartphones, tablet etc which is in route to the fog/CDMFC layer forming a peer-to-peer network as such smart devices are used by most of the peoples nowadays. Such peer-to -peer network can be realized through blockchain technology [18] which was officially used for bitcoin. Blockchains enable a smart device to become independent agents, autonomously conducting a variety of transactions. Data offloading is one of the important features of our CDMFC model. Through data offloading, the crowdsourced data securely reaches to the fog/CDMFC layer even if a direct link is not available. The procedural flow of our proposed CDMFC model explaining data offloading mechanism is clearly shown is Fig.2.

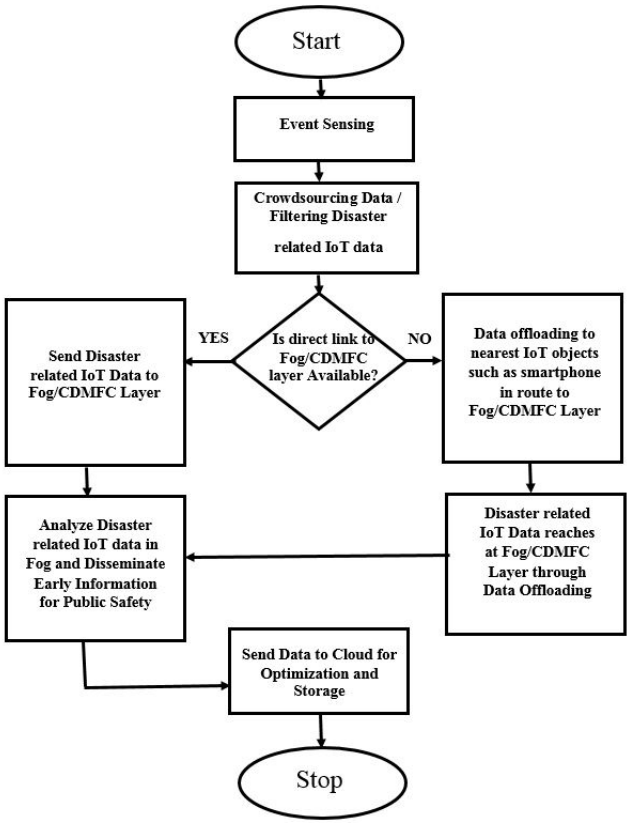

Fig. 2. Procedural flow of the proposed CDMFC model

C. CDMFC Model Layer

Through crowdsourcing and data offloading mechanism, the crowdsourced critical disaster-related IoT data is analyzed in CDMFC layer in a distributed way as we are taking advantages of fog computing. Here, the crowdsourced critical data is analyzed in real time and it minimizes latency unlike gigabytes of data are sent to the cloud for analysis directly from crowdsourcing layer. Nowadays, the data are generated with time and location stamps. The data generated through a various application such as Facebook and Twitter provides location and time stamps in real time. CDMFC model takes advantage of this feature to pinpoint the exact location and time of the disaster in a short period of time which is always crucial when the lives of millions of peoples are in danger. Further, in our CDMFC model, this layer is equipped with emergency contact numbers and is directly accessible to public safety authority who can plan rescue operation and take necessary action according to the crowdsourced critical disaster-related IoT data. All the multimedia applications related to disasters such as video, clips, photos etc. is saved in the fog and people of the affected region can easily see and efficiently realize the current situation. This could possibly save the bandwidth of the communication network. The cloud platform is also vulnerable to lots of attacks and security in IoT is a major concern. In CDMFC model, we can keep critical IoT disaster-related data inside the network and install our own security protocol for the safety of data. The use of fog computing and data offloading mechanism in our CDMFC model can efficiently realize machine-to-machine (M2M) communications, device-to-device communications (D2D) or human-machine interactions [19] through machine learning and human-aided machine learning techniques to further enhance the efficacy of the CDMFC model layer and it is the further interest of our future work. The data for long term storage and further analysis are sent to the cloud from CDMFC layer. It is widely known that many deaths during natural disasters are caused by the delayed or unprofessional response. Thus, CDMFC model layer acts as an efficient way to notify and analyze the disastrous situation in quick and detailed manner.

During such disastrous situation, it may disconnect a region or a complete country from rest of the world. CDMFC model layer can also trigger the drone-borne WiFi networks to provide the communication facility in the affected region or country.

D. Cloud Computing Layer

The non-critical data from crowdsourcing layer and other data from CDMFC model Layer are analyzed and stored in the cloud computing layer. In this layer, extensive data mining and visualization techniques are applied to arrive at a concrete

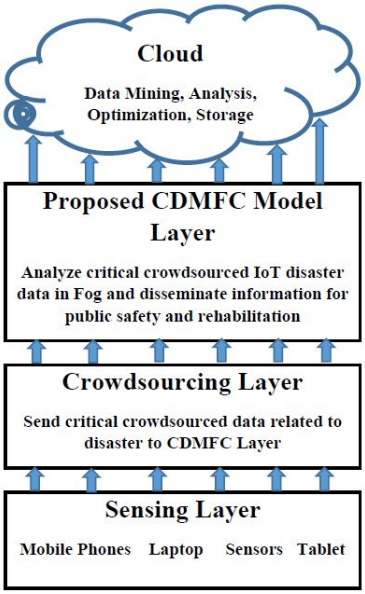

Fig. 3. Hierarchical layered structure of CDMFC model for disaster management

and final conclusion. Further, data are stored for a long time in the cloud for historical analysis.

IV. Conclusion and Future Work

Crowdsourcing the IoT data related to disasters can help public safety authorities to plan out efficient rescue operation and saves millions of people's lives struck in such dreadful situations. However, crowdsourcing data are often analyzed in cloud platform where latency will be quite high. The opportunity to act on the disastrous data might be lost when analyzing it in a cloud platform. Therefore, we need to minimize latency for better public safety and management during a natural disaster and emergency situations. Thus, in order to minimize latency and act on the data near to the place where it is generated, in this paper, we proposed a CDMFC model for disaster management. Our CDMFC model takes the advantage of fog computing platform where the critical crowdsourced IoT data related to disasters is analyzed in real-time. Further, we also propose a data offloading mechanism utilizing blockchain technology to send disaster-related IoT data to the fog/CDMFC layer if a direct link to the fog is not available. Through our CDMFC model, we can detect the disasters in real-time and plan out rescue operation accordingly. Moreover, our CDMFC model can conserve network bandwidth as the only disaster related data will be analyzed on fog and rest of the data will be analyzed in the cloud. Unlike cloud computing models which are often the target for attackers to manipulate the IoT data, CDMFC model can securely operate on the IoT data inside the fog where we can install of our own lightweight security algorithms.

In future, we plan to deploy the fog network and analyze crowdsourced IoT data in real-time. We will show the advantages of using fog computing and data offloading mechanism in a real-time dataset for our CDMFC model in minimizing latency and security concerns as compared to cloud computing models.

References

[1] C.-W. Tsai, C.-F. Lai, and A. V. Vasilakos, "Future internet of things: open issues and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2201–2217, 2014.

[2] S. Hasan and E. Curry, "Thingsonomy: Tackling variety in internet of things events," *IEEE Internet Computing*, vol. 19, no. 2, pp. 10–18, 2015.

[3] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Sensing as a service model for smart cities supported by internet of things," *Transactions on Emerging Telecommunications Technologies*, vol. 25, no. 1, pp. 81–93, 2014.

[4] A. Antonini, G. Boella, A. Calafiore, F. Cena, I. Lombardi, C. Salaroglio, L. Sanasi, C. Schifanella, and A. M. Soccini, "Sees@ w: Internet of persons meets internet of things for safety at work," in *Proceedings of the 19th ACM Conference on Computer Supported Cooperative Work and Social Computing Companion*. ACM, 2016, pp. 5–8.

[5] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and internet of things: a survey," *Future Generation Computer Systems*, vol. 56, pp. 684–700, 2016.

[6] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "Twenty security considerations for cloud-supported internet of things," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 269–284, 2016.

[7] M. Bhayani, M. Patel, and C. Bhatt, "Internet of things (iot): In a way of smart world," in *Proceedings of the International Congress on Information and Communication Technology*. Springer, 2016, pp. 343–350.

[8] F. Jalali, K. Hinton, R. Ayre, T. Alpcan, and R. S. Tucker, "Fog computing may help to save energy in cloud computing," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 5, pp. 1728–1739, 2016.

[9] M. Aazam and E.-N. Huh, "Fog computing: The cloud-iot/ioe middleware paradigm," *IEEE Potentials*, vol. 35, no. 3, pp. 40–44, 2016.

[10] E. J. Catlos, A. M. Friedrich, T. Lay, J. Elliott, S. Carena, B. N. Upreti, P. DeCelles, B. Tucker, and R. Bendick, "Nepal at risk: Interdisciplinary lessons learned from the april 2015 nepal (gorkha) earthquake and future concerns," *GSA Today*, vol. 26, no. 6, 2016.

[11] L. B. Brengarth and E. Mujkic, "Web 2.0: How social media applications leverage nonprofit responses during a wildfire crisis," *Computers in Human Behavior*, vol. 54, pp. 589–596, 2016.

[12] *Support Nepal Earthquake Survivors*, 2015, http://newsroom.fb.com/news/2015/04/support-nepal-earthquake-survivors-an-easy-way-to-donate-facebook-to-match-up-to-2-million/.

[13] A. R. Lee, A. Rauniyar, and S. Y. Shin, "Implementation of escarpment alarm system using terrestrial reference system," *International Journal of Future Computer and Communication*, vol. 4, no. 1, p. 72, 2015.

[14] B. Kantarci and H. T. Mouftah, "Trustworthy sensing for public safety in cloud-centric internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 360–368, 2014.

[15] L. Lambrinos, "On combining the internet of things with crowdsourcing in managing emergency situations," in *2015 IEEE International Conference on Communications (ICC)*. IEEE, 2015, pp. 598–603.

[16] H. Petersen, E. Baccelli, M. Wählisch, T. C. Schmidt, and J. Schiller, "The role of the internet of things in network resilience," in *International Internet of Things Summit*. Springer, 2014, pp. 283–296.

[17] Z. Xu, Y. Liu, N. Yen, L. Mei, X. Luo, X. Wei, and C. Hu, "Crowdsourcing based description of urban emergency events using social media big data," 2016.

[18] S. Higgins, "Ibm reveals proof of concept for blockchain-powered internet of things," *CoinDesk, January*, vol. 17, p. 2015, 2015.

[19] O. Said and M. Masud, "Towards internet of things: Survey and future vision," *International Journal of Computer Networks*, vol. 5, no. 1, pp. 1–17, 2013.