MOBILE EDGE COMPUTING BASED IOT WITH ONE TIME PAD ENCRYPTION

V.Shivadhar V.Srinivasan Prathima Devadas Kiruthiga Venugopal

Sathyabama Institute of Science and Technology.

ABSTRACT

We are in a period where Cloud platform and edge computing are becoming a major platform for the computation, processing of various data and communication between machines, sensors and smart objects, in real time applications and for many crucial tasks. With IOT expanding in various real time applications various techniques of implementing IOT are Emerging. It is important to understand the use of Edge computing which will provide methodology for information sharing, data processing, data storing and data analyzing. The applications of Edge computing in IoT is keep on expanding with improving technology in day to day life. This Paper is to assist and help researchers working in the area of the Edge computing platform to understand concepts involved in edge computing easily. This paper also explains standard instructions to be followed on how to protect messages with one-time pad encryption easily in simplest way and how to implement mobile edge computing based IOT with least use of resources.

KEY WORDS: MOBILE EDGE COMPUTING, ONE TIME PAD ENCRYPTION, SECURITY

INTRODUCTION

Computers and electronic gadgets are required whenever rate of correctness, automation, speed and accurate computations are needed. In the conventional computing system, the input is given by human beings and the software applications running at the systems processes the inputted data and produces an accurate output as possible. generally, the outputs are displayed on a output device such as a monitor or printer. As humans are lazy and there is possibility of inaccuracy in humans IOT systems are used. IOT Systems are 100 percent accurate and it eliminates possibility of human errors. The processing application is located at a central server in the case of an IoT system. The sensors in the IOT systems forward their data to a computing system via variety of networks such as mobile networks, Bluetooth, hotspot, WIFI, transmitter and receiver. The local computing system preprocesses all the data it obtains and sends it to a central server continuously using networks. In IOT an actuator or event-based notification system is used. Thus, an IoT system uses sensors, actuators and processors together to generate output. So IOT helps in improving automation in industries and cooperate companies. so we can summarize an IoT-enabled system is set of sensors, embedded system, electronics and communication devices which implements data storage via Internet into a cloud server and uses an analytics software to make decisions at the cloud platform uses help of analytics system to make certain decisions which is sent back to local device or end user. At periodic intervals, the collected data are analyzed using analytics software running in the server (cloud). The decisions and results from server are then informed accordingly to the end user. In most cases, it turns out to be the notification in the mobile device or actuation of some subsystems of the end device. We can use various technologies and concepts along with IOT. IOT can be implemented together with edge computing, fog computing, mobile computing and cloud computing or combination of these concepts. IN this paper we are going to see Different ways of implementing IOT with example system.

RELATED WORK

Wireless sensor networks consist of resource constrained devices that sense, process and transmit data from their surroundings to main server . They are launched in places that can be reached by humans. Due to their nature, many applications are available for their use such as health, military, monitoring and detecting abnormality in various cases[12]. Due to their computational speed, computational power and transmission constraints, the efficient use of sensors and resource constrained devices are essentially important. The mobile based communication, for example, places the highest strain on the energy conservation of the nodes [13]. Many related work has been done using edge computing concept in field of virtual reality and games[5] ,communication and networks[10] ,image processing[23].

EXISTING SYSTEM

IoT based remote monitoring systems are suggested by many professionals because of their reliability, time saving properties, accuracy and speed. In existing system, the IoT devices will keep observe the data from various resources and send data to the respective fog nodes for computation of health data. Then the computed values will be transferred to the cloud Server. Based on the abnormal condition the Cloud will send intimation to the clients. Use of fog nodes is not that efficient

as it makes the network complex and inefficient. This result in massive storage accumulation in cloud storage, processing the collected data is obviously a hard task to perform which results in computational overhead and delay in sending emergency alert.

PROPOSED SYSTEM

We propose the Secured OTP IOT Environment in Medical Field. Here the patient's android mobile device will be acting as the edge server for doing computing with the receiving data from health monitoring devices. The health-related data get uploaded into Mobile node. In Mobile Edge Layer, edge level computing is performed based on the threshold values the health status of respective patient is analyzed. If the status is getting abnormal then the Mobile Edge layer sends the health data with One-time pad security to the Cloud. Then the emergency SOS message will be sent immediately to ambulance, friends, close relatives, neighbors based on the type of event triggered. We propose in this system that the SMS is sent even without internet connectivity as it is for lifesaving and emergency purpose. Mobile computing promotes highly efficient output because maximum computation is done edge level which makes the cloud process as light weight. This system comes over the disadvantages of existing system and increase efficiency and decrease network and software requirements.

COMPARISON BETWEEN FOG COMPUTING, CLOUD COMPUTING AND MOBILE EDGE COMPUTING IN IOT.WHICH IS MORE EFFICIENT FOR PROPOSED SYSTEM?

IMPLEMENTATION USING CLOUD

Cloud provides data storage and hardware services virtually where the processing hardware is in random location. In cloud computing the data is sent to some data processor located in virtual location Where the data is processed and the result is sent back to the main server or the user application. This requires high speed internet and cloud service provider for cloud server which is time consuming and another problem is data maybe lost or easily hacked during tranctaction.For the proposed system high speed internet may not be available and it is required that in less time data is processed so implimenting using cloud is not much efficient .Availability is another problem with cloud. For the proposed system we need server available for 24/7 .In cloud we may have to send the data to randomly located long distance server in which there may be data loss during transfer and because of long distance data tranfer there are security issues .Data may be tampered with during tranfer .So cloud model is not considered for the proposed system.Cloud have security issues also.

IMPLEMENTATION USING FOG COMPUTING

Fog is a kind of distributed networking model that is closely associated with cloud computing and the internet of things. In fog computing multiple fog nodes are created each nodes are given individual data and each node process data individually and the data are combined and result is generated . Use of fog nodes is not that efficient as it makes the network complex and inefficient. This result in massive storage accumulation in cloud storage, processing the collected data is obviously a hard task to perform which results in computational overhead and delay in sending emergency alert. The huge disadvantage with fog computing is it cannot handle huge quantity of data continuosly .Implimentation and maintance of fog is complex.Comparing with requirements of our proposed system implementing using fog will not be much efficient .

IMPLEMENTATION USING MOBILE EDGE COMPUTING

IoT Mobile Edge Computing is a combination of tiny data centers locally placed where most of the data is stored and processed locally. These network of tiny data centers are connected in the form of tree, mesh, point to point, star topologies and they push the data received to a centrally located storage repository. The range supported is within a range of 10-meter square or less. So basically, Edge Computing is used for data analysis, storing and processing of data which are closer to the sensors that provide the data. Smart devices and sensors used in IoT Edge Computing are capable of processing critical data fragments and provide a quick real time response. These devices and sensors prevent the delay caused by sending the data through internet to cloud and back from cloud to local system. These devices also don't require high speed network. These devices are designed to act as small data centers that provides no latency. With this enhanced capability of Mobile edge computing, data processing is made to be implemented locally in decentralized server which effectively reduces the network traffic. This data can later be collected by the main server for further evaluation and processing. The data from the sensors or devices are sent to MEC Gateway (Mobile edge computing gateway) where the data is processed and analyzed to produce results. Mobile edge computing enhances the Cloud computing capabilities close to the Radio Access mobile Networks in 3G, 4G, 5G, LTE. CGSM, Bluetooth, ETSI is developing a system architecture and standard for a few Application program interface. Mobile edge computing manages local cache data local data breakout data analytics aggression. Virtualization in edge computing enables cloud computing providers to execute many independent application instances in a single physical server. In edge computing all the data is processed locally which is easier to manage. the user can track data and it is much secure and easy. This kind of architecture reduces complexity of implementation. The local device which process data can be made available 24/7 according to the usage of user The most important benefit of mobile edge computing is its ability to increase network

Approach	Edge nodes	Edge network
cloudlets	Compact size datacenters deployed on WIFI access	Wifi,3G,LTE
Mobile cloudlets	Compact size datacenters on cars	3G LTE
Multi access edge computing	Servers deployed in radio servers	3G,LTE,Other access technologies
Fog computing	Heterogeneous nodes including high end routers, access point setup box	Multiple wireless access technologies including WIFI,3G,LTE
Mobile cloud	Neighboring mobile nodes form a cloud with one device chosen as resource coordinator	Local networking through WIFI Bluetooth internet connectivity with wifi,3G ,LTE
Edge cloud	Compute or storage nodes deployed in edge network and federated to cloud data centers	Home/enterprise networks and WIFI hotspots
fusion	service nodes deployed on access points, local and centralized data centers	Not defined

Table 1- Different approaches in Edge

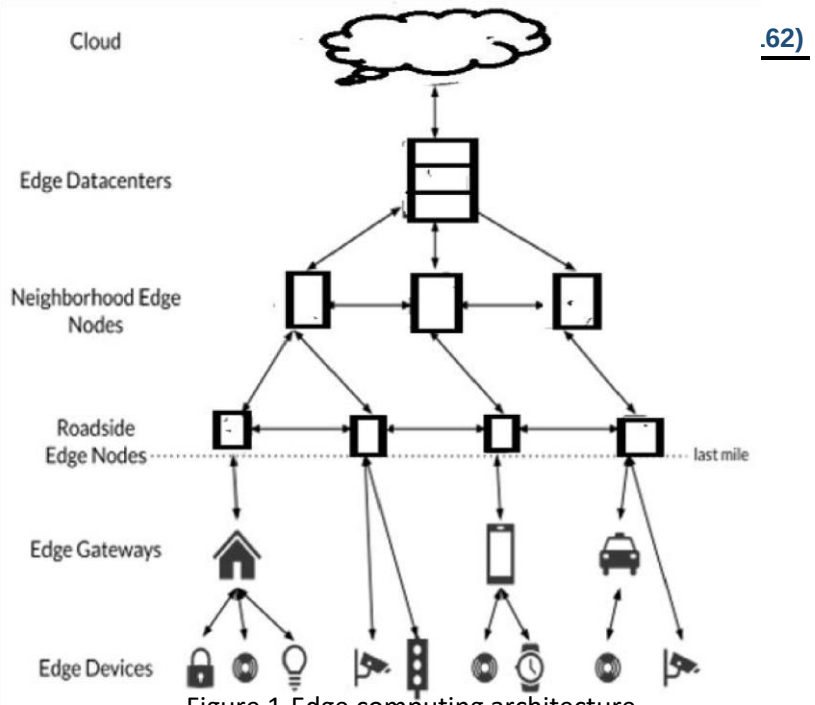

Figure 1-Edge computing architecture

performance by reducing latency. Since IoT edge computing devices process data locally or in nearby edge data centers, the information they collect doesn't have to travel nearly as far as it would under a traditional cloud architecture. Mobile edge computing could manage heavy network traffic so it is suitable. So we have considered to implement the system using this concept.

CLASSIFICATION OF EDGE COMPUTING PLATFORMS

There are three classifications (A)resource rich servers that are deployed at the edge level , (b) heterogeneous edge based computing nodes and (c) edge to cloud federation. The classification is based on how edge is deployed. However, in practice, one category can be used by combining one category with others categories. One category relies on servers with rich set of resources that are deployed very close(below 100 feet) to the end-devices. Another group uses the resources from various nodes present at the edge, including the end devices themselves. A third category is based on the federation of resources at the edge nodes and centralized data centers. each category Is explained below in detail

A)RESOURCE RICH SERVERS DEPLOYED AT EDGE:

One option to realize an edge computing platform is to deploy the resource-rich servers in the network to which end-users are connected A cloudlet is defined as a set of data centers that offers sets of clusters of multicore computing units, data storage and wireless LAN connectivity towards the edge .All the sensor data collected from sensors are processed on the cloudlet to provide real-time assistance and analysis assistance. Since the cloudlets are launched and introduced, further research professionals have proposed integration of cloudlets with femtocells, the LTE base stations define the architecture of micro data centers consisting of thousands of servers which are capable of hosting interactive applications for end-users. While these data centers have been used for deploying Content Delivery networks(CDNs) and email applications .they can also be reengineered to host cloudlets Similar to cloudlets which will be deploying a small set of servers on WiFi access points or a base station in the radio access network is called as a micro cloud.

B)HETROGENEOUS EDGE NODES:

In contrast to the set of techniques and solutions that are described above, edge computing platforms can produce a diverse set of computing resources. It consists of a fog platform devices (including smartphones and connected vehicles). Heterogeneity of wireless connectivity is a key aspect of the end-devices. Thus, many kinds of wireless access network(WAN) technologies are supported by their solution.fog computing is a cooperation based mobile cloud, wherein heterogeneous mobile devices opportunistically share their resources to deliver particular and appropiate services and applications which are characterized by a highly virtualized system of heterogeneous nodes, ranging from resource-rich servers to more constrained edge routers, access points, settop boxes and even end .

C) EDGE CLOUD FEDERATION MODEL :

Another option to understand edge platforms is based on the combination of computing resources at the edge and centralized data centers describe this concept as an edge cloud. In this system, edge applications are used to deliver services and resources at the edge as well as in distant cloud centers.

indoor 3D localization and video monitoring applications. Similarly, the correct combination of private and public clouds enable integrated IoT applications. In this Type of edge computing system, the edge node continuously orchestrates the federation of nodes to maximize the number of tasks that

to . All these informations will be saved into hospital server's database. We can use jsp to create web application easily. Java is a kind of programming language which has one of its major characteristic as a complete independence from the physical platform on the level of translated code. Java applet and java servelet page (JSP) can be used to develop Web pages distribute them to users . Using jsp we combine major java

are executed. For the fusion architecture in this model federation of cloud is important factor . In this edge model,the services are deployed on a cloud infrastructure which are then distributed throughout the Internet.

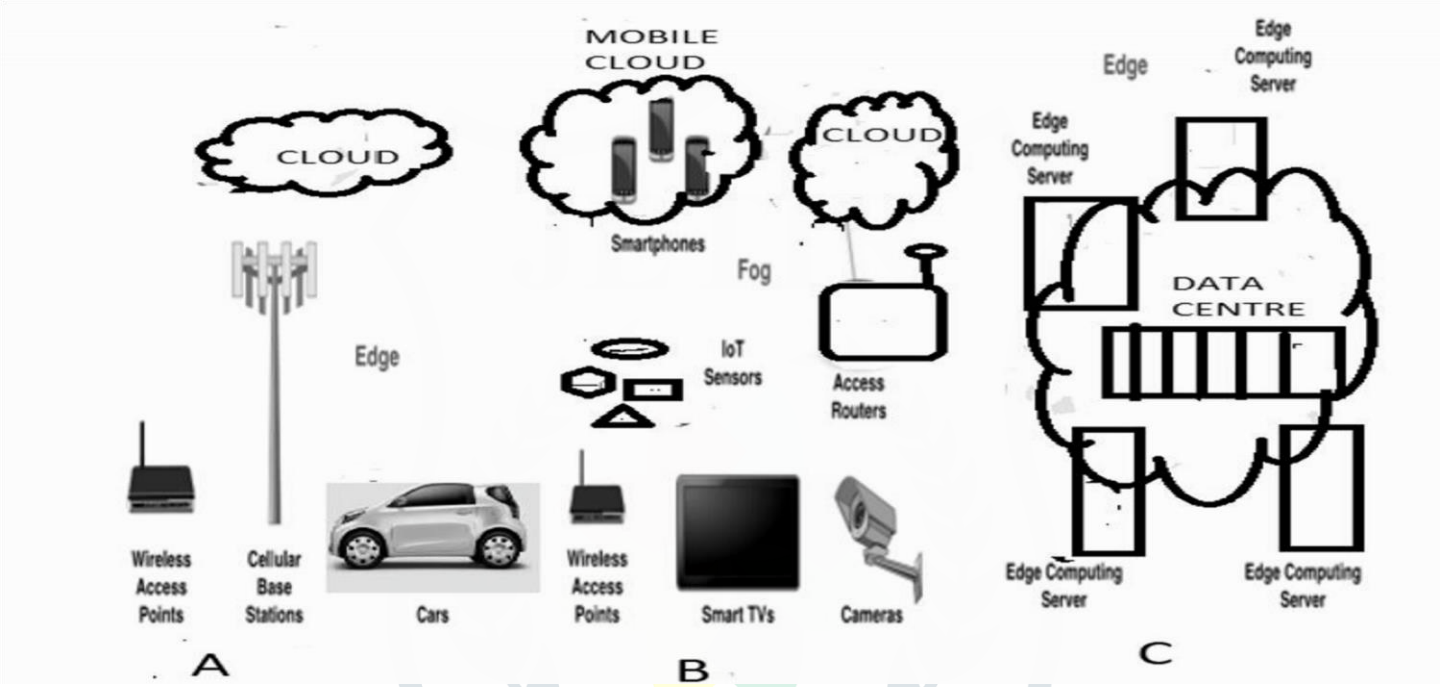

Figure 2 classification of edge models A)Resource rich edge server B)Heterogeneous edge nodes C)Edge-cloud federation

Many professionals advice the use of edge apps to launch

MONITORING HEALTH DATA USING EDGE BASED IOT WITH OTP

This project is to explain the practical implimentation of mobile edge computing based iot and otp encryption. We can split the project into 4 modules

1. User Authentication in Web-portal
2. Patient's Mobile Application and Appointment
3. Mobile Computation
4. Event Based Triggering

MODULE 1 USER AUTENTICATION IN WEB PORTAL:

In this module we have developed a web portal – Hospital Web application . Using this application new patients has to register their details and the data will be stored in hospital Server. Likewise a hospital Admin sign-in will be there they can add new doctors and specific specialist to which the doctors belong

concpts such as jdbc ,seing ,hibernate to create web server. The main features of java web applications are : it is recommended to code in advanded ide such as eclipse and netbeans.Because of the given features and reliability of java web development we implement the system using java.

MODULE 2 PATIENT'S MOBILE APPLICATION

In this module we create mobile application for patient this application monitors patient's health continuously and it maintains patient's health history .The patient communicates with this system by first registering his/her information at first instance by answering few questions related to health history and personal details. After registration is successfully done, a unique number for identification purpose is provided to the patient by the cloud server. To differentiate users, cloud layer provides identification such aspatient identification (PID) and the Server also provides sets of attributes related to health history of the patients. This module works in event triggered mode. In this mode, the requisite real-time sampled data is stored at the mobile nodes. The mobile edge layer will conduct

a data handling . Patients can request appointment to their respective Doctors from mobile application or web application.The mobile application can be easily developed for android using android studio using java concepts.

MODULE 3 MOBIL EDGE COMPUTATION

The health data from various sensors from respective areas will be processed in Mobile layer.We use edge-federation model of edge computing which is found to be efficient for this project implimentation.Patient's own mobile device acts as the main resource for computation. Based on the previous health dataset the computation will be processed. Data from different categories will be analyzed here. Health related data from previous history got collected from the Health dataset, Environment related data like air quality, noise level around the place where patient is, Behavior related data like whether the patient is having fits, vomiting, hyper tension, fainting etc. These kinds of data get analyzed in this layer.All these datawill be computed in the users mobile phone itself.The patient will be given watch like device will will consist of set of sensors these sensors will send the data to the patient's mobile application through mobile technology such as hotspot,bluetooth.These data are then computed in patients phone itself.All the defanitions and algorithms for the computations are defined in The patient's mobile application itself .The patient's mobile app generates a result and based on the result the application will conclude status of the patient based on critical values defined .The entire computation is controlled by the patient's mobile application .Hardware resources of the patients phone are primarily used for computation . After computing , the end result in form of report which is in text format will be sent to the one-time-pad security mechanism.The one time pad encryption and decryption will be implemented as given below.

ONE TIME PAD ENCRYTION

One-time pad encryption known as most secure and stable method to protect short text messages. This paper explains how to implement one-time pads, and how to deal with its various security issues. Working with one-time pads is easy to learn. The one-time -pad system is transparent and we dont need any computer, special equipment or any knowledge about cryptography techniques or mathematics .to impliment one time pad encryption . The system will surely provides unbreakable encryption when properly usedand implimented.

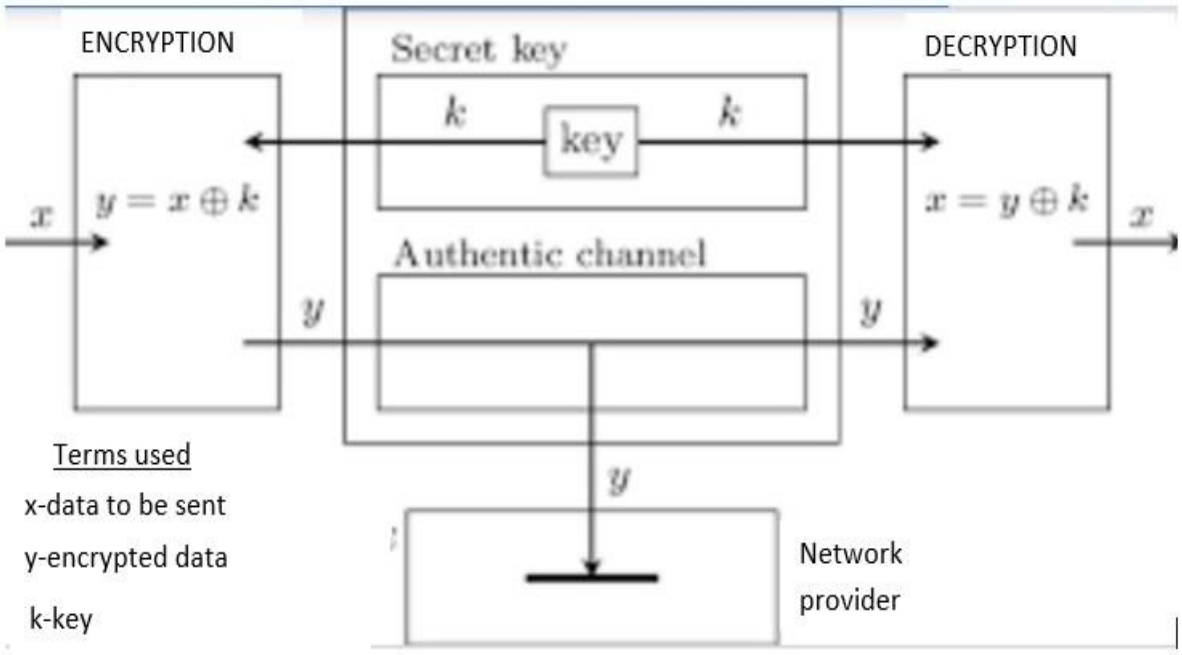

Figure 3-One time pad diagrammatic representation

It won't be possible to crack one-time pad encrypted data without having the proper key, even as future attack technology may evolve .The one-time pad (OTP), also called as Vernam cipher or the perfect cipher, is a cryptographic algorithm where plain text is combined with a random key to produce an encryted data. The OTP is uncrackable only if four important rules are followed. When rules are applied accurately, the one-time pad can be proven unbreakable. However, if any one of the given rules is not satisfied, the cipher is no longer unbreakable. The following

1. The minimum length of key is as long as the plaintext.
2. The technique of key generation is kept between the users.
3. There must only be 2 copies of the key: one key for the sending user and another for the receiving user (some exceptions exist for multiple receivers).

4. The keys are to be used only once, and both sending user and receiving must destroy each of their keys after use

IMPLEMENTING ONE TIME PAD ENCRYPTION

To perform one-time pad encryption we need a key, called one-time -pad- key.The key is generated based on random technique users choose . One-time pad encryption is only possible if both sender and receiver are in possession of the same key which needs to be communicated or technique of key generation has to be known by the users. Therefore, both sender and receiver must exchange their keys beforehand and be ready. one key could be sufficient for a very long period as long as it is kept secret by users.

ENCRYPTION

To perform encryption First covert all data to hexadecimal and store it in variable.we get the key from length of data.perform XOR operation between the data and key to get the encrypted data. Now the data is completely secure ciphertext! Let us see an example with medical data

Bp 110

Pulse 65

1)hexadecimal form of above data

4270313130

50756c7365203635

2)key(length=26)

3236

3)encrypted data

4270310306 50756c7365200403

the message is sent by radio, in voice or Morse, or by telephone, or SMS .it is recommended to relay all groups twice to avoid problems.

DECRYPTION

Write the one-time pad digits underneath the ciphertext and add ciphertext .Perform operations from encryption in reverseorder . Calculate key from encryted data. Here the technique used to generate key is nothing but finding the length of data therefore the key is equal to length of data perform reverse xor operation of encrypted data with key to get final data. Let's see an example.

1)encrypted data

4270310306

50756c7365200403

2)key calculation

Length=26=3236

3)decryption(reverse xor)

4270313130

50756c7365203635

4)hexadecimal to text

Bp 100

Pulse 65

After decryption the receiving user can successfully view the message .

We create the encrytion in the application itself . The application automatically encrypts the data .We are create the encryption algorithm using arithmetic and bitwise operators in java concepts.The

MODULE 4 EVENT BASED TRIGGERING

This is Stage where alert SMS is sent to patient's known members and ambulance.The members to whom the SMS containing patients health report is to be sent is decided based on the result of the patient's status.The status and health report sent will be in encrypted format. When the mobile device performs computation periodically when the values got reached above the threshold value then it will detect that patient is in emergency state and has abnormal condition. So spontaneously the mobile node will send the abnormal data to the Cloud in encrypted format and here the Event is triggered by the cloud server. The Emergency alert to the Doctors, medical team, ambulance, relatives, etc . Thus the alert will be sent to respective mobile users. Set of actions are done according to the result from edge computation.At the receiver end the user has to click the received text and enter the key to obtain the original text. The main task of this module is to choose the members whom are supposed to receive the SMS.This module chooses the members that should receive the message based on the result .

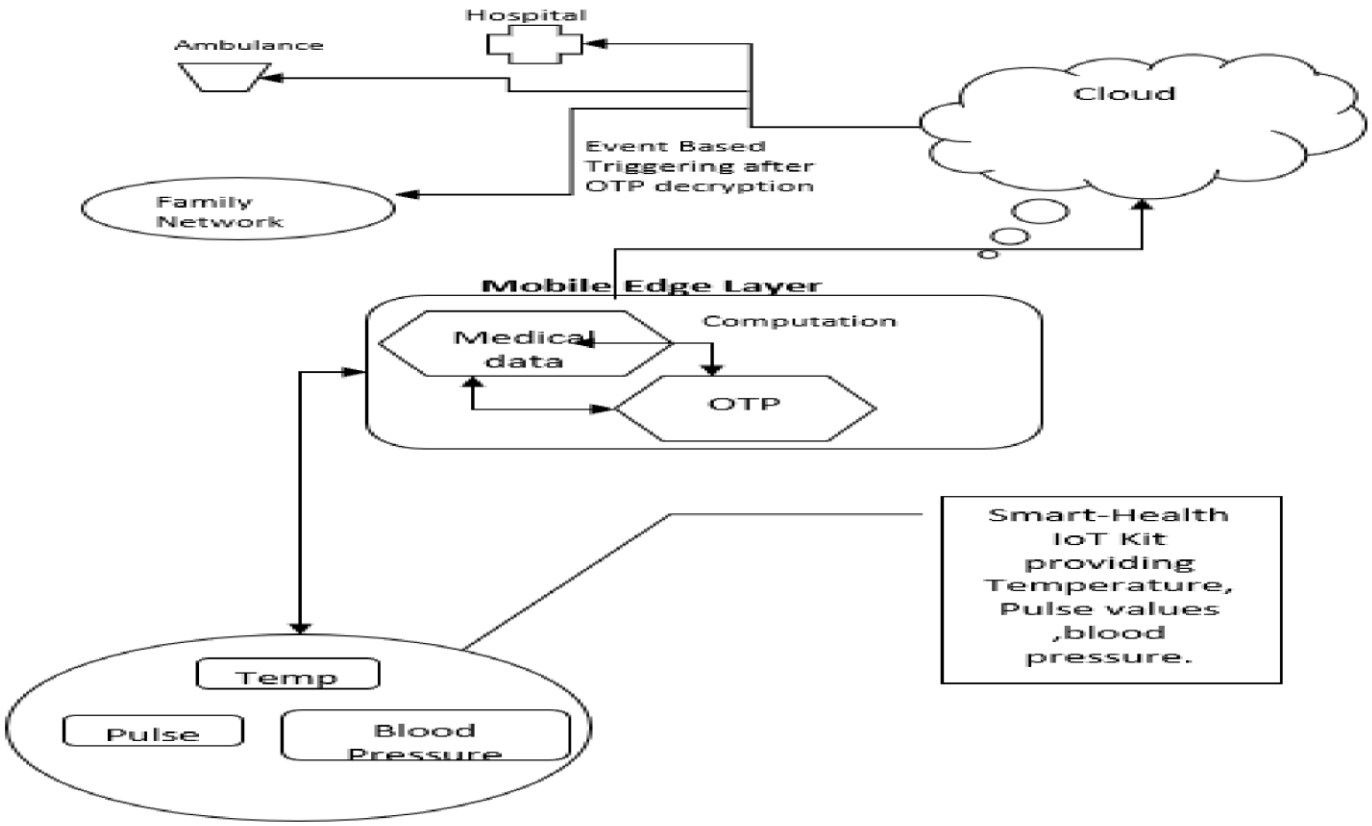

Figure 4 – Proposed System Architecture

SUMMARY AND CONCLUSION

Hence in this paper we have evalvated the sustanability and efficiency of edge computing using mobile networs. Specifically, we evaluated the performance of edge computing in health care application as aa example system to understand the mobile edge concepts in deep . the end results have shown that edgecomputing is necessary for efficient less resource oriented and fail free system in health application and other cases . Although regional data centers allow to significantly reduce network latency, only hosting resources at the edge enables a satisfactory quality of experience for proposed system. Furthermore, increasing the computational capabilities of the servers in the cloud does not compensate for the increase in network latency. Therefore, deploying even limited computing resources at the edge helps improve the quality of experience in the considered system. We hope that this article will encourage further research in this direction and evolve the edge computing technology further

REFERENCES

[1] R. Li, H. Harai, and H. Asaeda, “An aggregatable namebased routing for energy-efficient data sharing in big data era,” IEEE Access, vol. 3, pp. 955–966, 2015.

[2] R. Li, H. Asaeda, and J. Li, “A distributed publisherdriven secure data sharing scheme for information-centric iot,” IEEE Internet of Things Journal, 2017.

[3] M. Satyanarayanan, P. Simoens, Y. Xiao, P. Pillai, Z. Chen, K. Ha, W. Hu, and B. Amos, “Edge analytics in the Internet of Things,” IEEE Pervasive Computing, vol. 14, no. 2, pp. 24–31, Apr.-June 2015.

[4] K. Ha, Z. Chen, W. Hu, W. Richter, P. Pillai, and M. Satyanarayanan, “Towards wearable cognitive assistance,” in Proc. 12th Int’l. Conf. Mobile Systems, Applications, and Services, Bretton Woods, NH, June 2014.

[5] S. Liszio and M. Masuch, “Designing shared virtual reality gaming experiences in local multi-platform games,” in International Conference on Entertainment Computing. Springer, 2016, pp. 235–240.

[6] J. Farman, “Locative life: Geocaching, mobile gaming, and embodiment,” Digital Arts and Culture 2009, 2009.

[7] S. Chess, "Augmented regionalism: Ingress as geomediated gaming narrative," Information, Communication & Society, vol. 17, no. 9, pp. 1105–1117, 2014.

[8] E. Graells-Garrido, L. Ferres, and L. Bravo, "The effect of Pok´emon Go on the pulse of the city: A natural experiment," arXiv preprint arXiv:1610.08098, 2016.

[9] ETSI, "Mobile-Edge Computing Introductory Technical White Paper," Sep. 2014.

[10] T. Nishio, R. Shinkuma, T. Takahashi, and N. B. Mandayam, "Service-oriented heterogeneous resource sharing for optimizing service latency in mobile cloud," in ACM Proc. 1st Int'l. Workshop Mobile Cloud Computing & Networking (MobileCloud '13), Bangalore, India, July 2013.

[11] H. Chang, A. Hari, S. Mukherjee, and T. Lakshman, "Bringing the cloud to the edge," in IEEE Conf. Comp. Comm. Workshops (INFOCOM WKSHPS), April 2014.

[12] P. Mach and Z. Becvar, "Mobile edge computing: A survey on architecture and computation offloading," IEEE Communications Surveys & Tutorials, 2017.

[13] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," IEEE Communications Surveys & Tutorials, 2017.

[14] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On multi-access edge computing: A survey of the emerging 5g network edge architecture & orchestration," IEEE Communications Surveys & Tutorials, 2017.

[15] P. Simoens, Y. Xiao, P. Pillai, Z. Chen, K. Ha, and M. Satyanarayanan, "Scalable crowd-sourcing of videofrom mobile devices," in Proc. of the 11th annual International conference on Mobile systems, applications, and services. ACM, 2013, pp. 139–152.

[16] A. Greenberg, J. Hamilton, D. A. Maltz, and P. Patel, "The cost of a cloud: research problems in data center networks," ACM SIGCOMM computer communication review, vol. 39, no. 1, pp. 68–73, 2008.

[17] S. Wang, R. Urgaonkar, T. He, M. Zafer, K. L. Chan, and K. K. Leung, "Mobility-induced service migration in mobile microclouds," in Military Communications Conference (MILCOM), 2014 IEEE. IEEE, 2014, pp. 835–840.

[18] K. Hong, D. Lillethun, U. Ramachandran, B. Ottenw¨alder, and B. Koldehofe, "Mobile fog: A programming model for largescale applications on the internet of things," in Proceedings of the second ACM SIGCOMM workshop on Mobile cloud computing. ACM, 2013, pp. 15–20.

[19] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," IEEE Internet of Things Journal, vol. PP, no. 99, pp. 1–1, 2016.

[20] L. Canzian and M. Van Der Schaar, "Real-time stream mining: online knowledge extraction using classifier networks," IEEE Network, vol. 29, no. 5, pp. 10–16, 2015.

[21] Y. Elkhatib, B. Porter, H. B. Ribeiro, M. F. Zhani, J. Qadir, and E. Rivi`ere, "On using micro-clouds to deliver the fog," IEEE Internet Computing, vol. 21, no. 2, pp. 8–15, 2017.

[22] I. Farris, L. Militano, M. Nitti, L. Atzori, and A. Iera, "Federated edge-assisted mobile clouds for service provisioning in heterogeneous iot environments," in Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on. IEEE, 2015, pp. 591–596.

[23] A. R. Elias, N. Golubovic, C. Krintz, and R. Wolski, "Where's the bear?-automating wildlife image processing using iot and edge cloud systems," in Internet-of-Things Design and Implementation (IoTDI), 2017 IEEE/ACM Second International Conference on. IEEE, 2017, pp. 247–258.

[24] ONF, "Software-defined networking: The new norm for networks," ONF White Paper, 2012.

[25] K. Kumar, J. Liu, Y.-H. Lu, and B. Bhargava, "A survey of computation offloading for mobile systems," Mobile Networks and Applications, vol. 18, no. 1, pp. 129–140, 2013.

[26] Internet of Things for Smart Cities Andrea Zanella, Senior Member, IEEE, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, Senior Member, IEEE, and Michele Zorzi, Fellow, IEEE

[27] V.R.sarma Dhulipala ,Prathima Devadas and P.H.S Tejo murthy -Mobile phone Sensing Mechanism for Stress relax using Sensor Network. Wireless Personal Communication

volume 86,page 1013-1022(201