A Secure Internet of Things based Smart Monitoring System

Bhabendu Kumar Mohanta, Debasish Jena

Abstract: ***Internet of Things (IoT) is a connection of interconnected any things deployed in different applications. The IoT is emerging as a technique for real-time monitoring the environment like Earthquake early detection. Snow level monitoring, forest fire detection, Gas level monitoring in a Smart Kitchen. IoT based sensor network need secure communication, processing, analytics and transient storage for better monitoring of smart environments. In this article, the authors proposed a secure framework for data collection and further processing from the sensors network to the core of the network using Fog-Cloud based architecture. The paper implemented the proposed framework taking different sensors deploy in an IoT based smart kitchen environment. For experimental purpose, Raspberry Pi used as a fog node and local cloud server to monitor the environment in real-time, SQLite is used as buffer storage. The experimental setup and result show that the proposed framework is secure to monitoring in a sensor network.***

Index Terms*: *IoT, Smart Monitoring, Security, Computing.

I. INTRODUCTION

Internets of Things (IoT) device are Predictable to cross 50 Billion as estimated by CISCO [1]. As the number of IoT devices are developed and deployed in a different application. IoT has much application out of which monitoring of environment is one of the most important. The different sensors are used to detect the environment condition. Smart monitoring means real-time reading the input and responding to the situation in a quick time. A lot of application are like health monitoring, earthquake detection, _re detection in kitchen, gas leakage need to securely create network and process in real time. IoT based framework used to monitor the leg movement to detect the arthritis disease [2] which will prevent the serious fatal or even death to the patient. In a smart environment monitoring system collecting the information and processing in real time is very much important. The processing the information in the edge of the sensor network instead of a cloud environment can save the latency time as well as bandwidth. Many applications are like monitoring of train safety in automatically [3], Chemical monitoring [4], Gas leakage monitoring [5{7] recently develop for Monitoring based on IoT and Cloud Computing concept. As shown in figure 5 IoT application has three basic layers.Sensors and actuator are deployed in an environment to capture the information. In the recent past, some work is done on monitoring the system using a technique like Wireless sensor network, Software define network, Cloud computing.

The processing of the collected data are in a remote server or cloud server. Doing computation in the cloud increases latency and bandwidth. The rapid growth of IoT enable device deployed in a large number of applications generated a huge volume of data. In a real-time monitoring system if the information is read in each second from sensors devices then it creates a substantial memory space, processing, and communication bandwidth. The cloud computing provides all the resource and can processing huge volume of data but it takes some amount of time. As some of the IoT applications requiring fast response, some having involves private data where a user is not interested to send his credential to the cloud server. If locally data are store and process it will create a problem for the network[8]. The integration of cloud computing with IoT is attractive because of some benefits. But most of the IoT problems are remain same as time delay, location awareness, bandwidth issue. The cloud computing being centralized system access remotely by the IoT for which latency increases in the network[9]. As in the smart environment monitoring system where IoT devices and end users need to access the information and services in real-time which is not supported
by the cloud platform. So there is a demand to have a novel technology which will address the storage and process at the end of the IoT application. The fog computing can bring the services nearer to the end users. The fog computing technique nothing but the the extension of cloud means it has processing power and storage capacity.
Some of the important properties of fog computing are [10]:

- Low Latency
- Large scale applications
- Mobility of devices
- Decentralization
- Low capacity of device
- Location Awareness
- Geographic Distribution

A. Contribution of the paper

- The authors propose a Fog and Cloud Based architecture for local data processing using fog computing.
- Integration of Fog computing in internet of things are explained in details.
- The security issues in IoT system are identified in this work related to smart monitoring system.
- The experimental results show the real-time monitoring of the smart system is capable of analyzing the data and produces corresponding events.

Revised Manuscript Received on July 05, 2019.

Bhabendu Kumar Mohanta, Computer Science and Engineering, International Institute of Information Technology(IIIT), Bhubaneswar, India.
Debasish Jena, Computer Science and Engineering, International Institute of Information Technology (IIIT), Bhubaneswar, India..

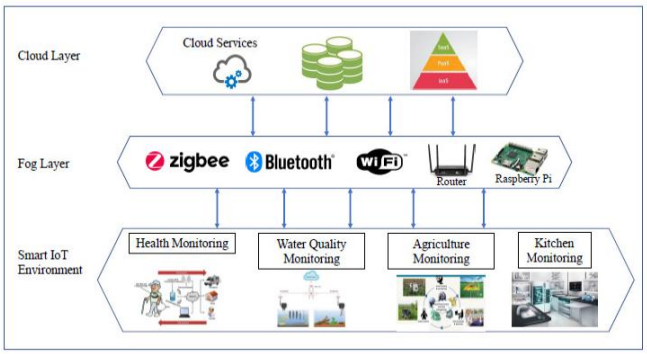

Figure 01: A general Three-layer Architecture of IoT Application

B. Organization of the paper

The recent related work on the different monitoring system is study briefly in section 2. The fog based system model proposed in section 3. The integration of fog computing with the IoT is explained in section 4. In section 5, the experimental setup and result analysis are done. The paper concludes with the future work in section 6.

II. Related Work

A low-cost sensor network system implementation to monitor crucial parameters in an indoor environment is proposed in the paper [11].To provide a improved risk management strategy to prevent causalities in a Reinforced Concrete (RC) and masonry building during earthquake and floods, a monitoring system is proposed in paper [12] which screens the health of the structural elements in RC and warn the authorities if there is any physical damage. The paper [13] has presented a water quality monitoring system using WSN to supply clean and safe water. The laborious, time consuming, ineffective method of conventional monitoring process which involves a long procedure, from collecting the samples manually and to send them to laboratory for analysis to get the results which are not real-time in nature has been replaced by an alternative process based on WSN which are very affordable and can be operated remotely and provide real-time results with least human intervention. In paper [14] a hierarchical routing protocol for water quality monitoring of river or lake is proposed by deploying a huge number of inexpensive sensor nodes in a large area using hierarchical communication structure, which reduces the overhead in communication and increases the life span of WSN as compared to LEACH, its predecessor. To monitor the traffic volume, performing vehicle classification, an IoT based wireless sensor system is presented in this paper [15].In the paper [16] a WSN based monitoring system to monitor Soil quality parameters such as humidity, temperature, acidity, and conductivity is proposed. A wearable smart sensor device is designed in the paper [17]for an elderly person which can detect the accidental falls of the person by monitoring the treble, using consumer home networks. The paper [18] proposed in-pipe monitoring and on-the-fly assessment of water quality in real time for drinking water distribution system by using low-cost sensor nodes. A real-time damage detection application by using an open source data analytics WSN called Snow Fort is used for structural health monitoring is proposed in the paper [19].The paper [20] introduced two resolutions which are not equally exclusive by analyzing two usual situations involved in seawater quality monitoring. The system is based on Decision Support System (DSS). The first solution is to monitor the isolated spots and the second one is an extended of first one for the cases where an advanced special resolution is required.[21] As an extension of WSN underwater atmosphere, underwater acoustic sensor networks (UASNs) emerge as anxiety of academia. In an ocean application where the water level is very deep efficiency and reliability of UASNs technique is very challenging for data transfer to monitor any unusual submarine oil pipelines.

The paper [22] has proposed a health monitoring system for diagnosis and anticipating medical stress. The proposed system not only monitors with accuracy but also provide the feedback to the user. On identifying the medical stress, it also sends a notification to a medical doctor. A system for real-time monitoring and detecting concentration of Carbon Dioxide through Cognitive WSN in an indoor environment is presented in the paper [23]. It also sends an alert with overall air quality details in a timely manner. The author has presented a literature survey based on the gas diffusion models used for measuring the gas concentration in the large area and also provided a comparative study between continuous object localization and boundary detection schemes in the paper [24] considering the complexity, estimation accuracy and energy consumption as parameters. The paper [25] proposed a Cattle health monitoring system based on wireless sensor network which monitors the feeding and drinking behaviour of the animal. Use of directional antenna in the proposed system allows one router for simultaneous monitoring of multiple animals along with an efficient mesh routing protocol for aggregating the monitored data. An ECG monitoring system based on home-based wireless network i.e. Zigbee has presented in the paper [17], which not only monitors the health of the people in their own home but also can be monitored by the physician periodically for providing appropriate healthcare.The most of the related research based on wireless sensor network.The WSN being the ad-hoc type of network it even connected with wireless access point it associated with some issue.

III. Proposed System Framework

The overall architecture of the secure sensor network for environment monitoring system is shown in the Fig.02. The components are various sensor such as gas, temperature, camera, many raspberry pis as local nodes and one raspberry pi as cloud server. The designed IoT based smart environment monitoring consists of 3 layer design for monitoring, storing, processing and data visualization.

A. Layer 1 : Monitoring and Data Collection

In Layer 1 data monitoring takes place using various sensors such as MQ gas sensors which monitors various gas constituents values in a room hence stating the the quality of air in that room, temperature and humidity sensors (DHT22), an infrared camera to keep track of any movement in the room deployed in the environment.

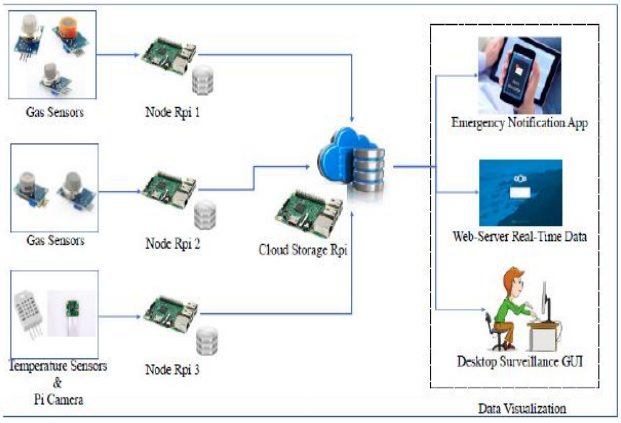

Figure 02: Proposed System architecture for Smart environment

B. Layer 2; Data Storage and Processing

Layer 2 is for storing the data collected through the sensors. First the data will be stored in a local raspberry pi. The node raspberry pi that keeps the system of sensors up and running, stores the data in the local database for a buffer time of 4hrs for backup. The local databases are synced with the central database on the cloud. For a cloud database, another raspberry pi is configured.

C. Layer 3; Data Visualization

Layer 3 involves the data visualization which can be done in three ways in this particular application. The real time data and chart insights are shown in the nextcloud API for monitoring sensor logger. A desktop based Python GUI ensures overall surveillance of the Server room at all time that syncs with the cloud for all details and back-end data.
A mobile app signals on any sort of emergency or alert for the spikes in data charts that surpass normal parameters

D. Pseudo Code

Algorithm 1: Initialization and Monitoring

Step 1: Deploy the gas and temperature sensor in the monitoring environment
Step 2: Constantly measures the temperature and the gas constituent values such as CO, CO_2, LPG in terms of PPM(parts per million) in the room.

Algorithm 2: Setting up Local and Cloud Storage

Step 1: Install SQLite on Raspberry Pi connected to IoT sensor for buffer storage of sensor data.

Step 2: Configure one Raspberry Pi as Web server by installing Apache on it.

Step 3: For processing of PHP files, Intsall PHP module for Apache.

Step 4: Install and configure Uncomplicated Fire Wall(ufw) to secure the R-Pi.

Step 5: Install Fail2Ban on the Raspberry Pi to add another layer of security

Step 6: Install Nextcloud to make it as a personal cloud server

Step 7: Add SensorLogger API on the NextCloud to log the sensor data and get chart insights in real-time

Step 8: Install MySQL on cloud server for persistent data storage.

Algorithm 3: Data Visualization

Step 1: Initially all the sensor nodes deployed in the environment sends a registration request to cloud server.

Step 2: Implement ECC for encryption mechanism.

Step 3: On successful registration of the device, add the device id on NextCloud server to monitor the data through an url.

As explained in pseudo-code different algorithms for initialization, setting up the storage and data visualization. In Algorithm 01. Sensors are deployed and connected to the fog node. The fog node has the capacity to process data and store with its limited storage. In this work, SQLite installed in fog devices to store the collected information from different sensors. After every 4hrs the information is forwarded to the cloud. All the system configuration and storage space are created using the local cloud in Algorithm 02. The registration of all the sensors in the cloud server is done through fog node. The device is added to the next cloud to monitor the data explained in Algorithm 03.

IV. INTEGRATION OF FOG COMPUTING WITH IOT APPLICATION

The proposed framework has sensors node connected with the Fog node for further processing the data. Fog computing provides computing and storage at the edge of the end users. It is the extension for cloud computing. In IoT application like the smart healthcare system where patient health condition monitoring needs to be done in real-time. if the processing of composed data is sent to the cloud for additional analysis then there will be time delay which may cause serious damage even death to the patient. so in that situation, if the analysis is possible done in at the network end side that quick action can be taken.
In the smart environment monitoring system also demand processing and analysis must be done in quick time so that appropriate action should be taken to avoid any damage.The smart environment means consists of smart devices capable of sensing and sending the environment value to the corresponding authority. The emerge of IoT in last decade lots of devices are manufactured with not only sensing the environment even has the capacity to connected to other devices through Wireless as well as wire and send notification if some events occur.
Fog computing can be a integral part of IoT application implementation. It provides computing at the end of the network. The fog computing supports virtualization. Fog computing largely depends on cloud computing means fog cannot work separately like Mobile edge computing

or cloudlet [26]. Fog has some of the properties which enhance the IoT application like Resource Sharing, Task Scheduling, Offloading and Load Redistribution.

A. Resource Sharing: In the fog system when the computation is done at the fog layer. The multiple fog node can take part in the computing process to make the decision more efficient and reliable to the network in a cooperative and distributed in nature. As a centralized decision-making process more vulnerable to the outside world and the single point failure may occur. as in a smart environment monitoring case, the system must not fail due to any reason. so computation and sharing of the resource must be done in a distributed and cooperative manner some of the work has been there which address the issue [27-29]

B. Task Scheduling*:* In a larger IoT application where more number of fog devices are connected for computing. There must be some scheduling algorithm for assigning the job as per the demand as well as the priority of the job. Using the task scheduling fog devices are perform computation in a cooperative way.

C. Offloading and Load Redistribution*:* In a fog computing environment, all the fog node may not be available all the time to participant in the computing process. So the load of the network must be distributed in such a way that execution of the task completed in due time. so that the reliability of the network can be maintained. If any fog node becomes offline due to hardware failure or any other reason other nodes must take up the job execution and completed the task.

V. SECURITY ISSUES IN IOT APPLICATION

Internet of Things (IoT) does not have a standard security protocol till now. The use of IoT concepts is most emerging in many applications. The basic architecture of IoT consists of three layer, physical layer, network layer and application layer. IoT need to ensure the security in each layer. Some of the securities issues are:

A. Authentication

In the IoT application, device identification and actual user identification is essential. Once the application is setup IoT devices can sense the environment and send to the corresponding nodes for further processing if any unauthorized nodes get the information then the whole system become use less. To perform computation and processing in secure way all the nodes must authenticated using some authentication technique. So that IoT applications can perform all the communication and processing of information in securely. Authentication is very much important.

B. Authorization

As IoT devices are resource constraint devices means they have less storage capacity and less processing power. So communication between devices and processing of information must be done with specific node. The proper accessibility must be assign to the corresponding node using some access control mechanism. So that authorization is maintained in the system. The information is share only to the authorize node only.

C. Man in the middle attack

In an IoT application communication between different entities need to be done securely. Otherwise, when communication takes place between two IoT devices the attacker can read the information in the middle of the communication channel and perform modification of the information and send to the other end. Sometimes it reads only the information; later on again send the same information in the system behavior like a normal user. So man in the middle attack is a security issue to the IoT system. Its need to be address, so that the communication can be done in a reliable medium.

D. Denial of Service (DoS) Attacks

DoS attack is a type of cyber-attack which tries to exploit the "availability" part of CIA Triads making the server inaccessible to its users. The attacker tries to flood the server with huge amount of traffic which results in compromising with the resources and bandwidth. Although DoS attack don't results in loss of sensible information but these cost a huge amount of loss for the victim.

E. Trust management

IoT application like smart home, smart healthcare system, smart city where users give his/her personal information to the system. The system architecture must be design in such a way known his/her information is protected or privacy is maintained. For example in a medical records of a patient must be maintained no one want their personal information is available to the all users in the system.similartly in a smart home case whatever happening in sa smart home should not be available to the others person who are not belongs to that smart home system. So to implement the smart system using IoT trust management is one of the most important issue need to be address.

F. Confidentiality

In an IoT network as large numbers of sensors and IoT enable devices like fog node or edge node are used for real-time processing of data at the edge of the network. The confidentiality of each node must be maintained. Otherwise sensitive information of the nodes may be hack by the attacker.

G. Availability

In IoT system different resource constraint devices are deployed to get the information from the environment. As the devices having less power and less storage devices, the storage and processing is an issue in IoT devices. Similarly the connectivity is done either wire or wirelessly. To get information from the environment device must have connected to the network layer all the time. So the availability of the devices is also an issue in IoT system.

H. Data Transit Attack

In this type of attack, the attacker targets the communication medium. They monitor all the packets passing through a given network and tries to exploit it. The most common data transit attacks are sniffing attacks and Man-in-the-middle (MITM) attack.

I. Non-Repudiation

Non-Repudiation means denying the authenticity of any transaction or operation done in a system. This type of attack possible when there is no proper authentication or log file maintained in a system. In an IoT system, lots of sensitive information flows between different nodes, so the system needs to have proper authenticate process.

J. Malicious Attack

In this type of attack, the attacker tries to execute a malicious code into an application running in victim's system as a result of which the attacker is capable of compromising database integrity, privacy, and security.

VI. EXPERIMENTAL SETUP AND RESULTS ANALYSIS

In Fig.03 shown that the proposed system framework in laboratory views. Different sensors are connected to the Raspberry Pi(fog node) device. The system configuration consists of the breadboard, wires, ADC and sensors. For this work different type of sensors like DHT22, MQ6, MQ9, MQ3, and MQ135 is used to monitor the smart environment. For build up the IoT devices and to read the value python programming language is used.

RASPBERRY PI 3 MODEL B+ used as a fog node. These fog nodes can access the different sensors deployed in a smart room environment. RASPBERRY PI module have specification like Broadcom BCM2837B0, Cortex-A53 (ARMv8) 64-bit SoC @1.4GHz, 1GB LPDDR2 SDRAM 2.4GHz, and 5GHz IEEE 802.11.b/g/n/ac wireless LAN, Bluetooth 4.2, BLE. One high-end device having fully tamper-proof having large storage and high processing power used to authenticate the entire fog node. SQLite Version 3 is installed on the RASPBERRY PI used as buffer storage with a buffer time of 4hrs. In case of any connection failure to cloud server within buffer time, the sensor data can be retrieved and again synced up with the cloud server once the connection is up and running.

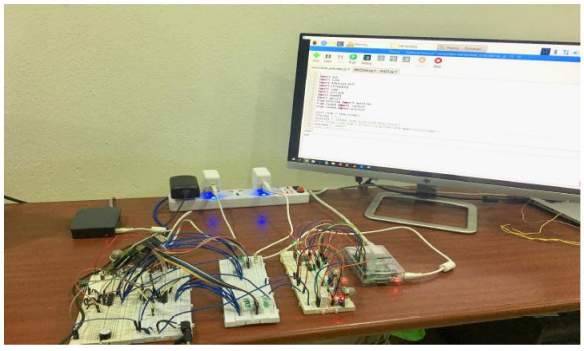

Figure 03: Proposed System architecture of Smart environment: laboratory View.

As shown in Fig. 03 initially to test the smart environment, we have deployed different sensors devices and done the experiment.

In Fig. 04 devices are authenticated with a proper identity are shown. Similarly in Fig.05 Dashboard of the smart environment is shown. In the dashboard all the statistical information are shown to the authenticated devices.

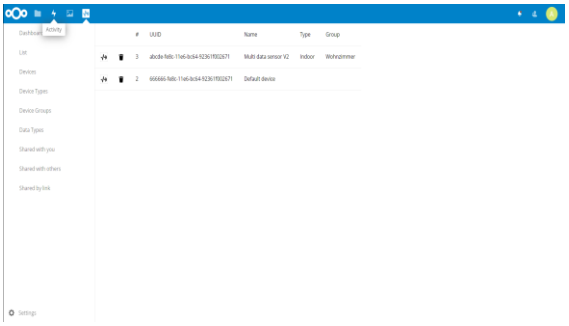

Figure 04: The GUI of Device identity

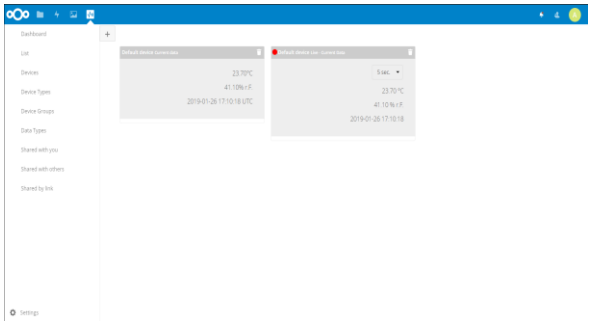

Figure 05 : The GUI for data collection(Dashboard) from Smart environment

As shown in Fig.06 we have tested the system in scenarios: 1) Outdoor environment 2) Indoor Lab environment 3) In presence of some flammable gas. The values of CO(in PPM) at a different time in different scenarios can be shown from the graph. We have considered the same testing scenarios as CO gas monitoring for CO2 gas , LPG gas monitoring and shows the result of temperature monitoring data using DHT22. The normal temperature of the room varies between 16^0 Celsius to 35^0. if a sudden rise and steady high value of temperature noted by the sensor, an alert message is sent to the user phone to notify them about this abnormal situation.

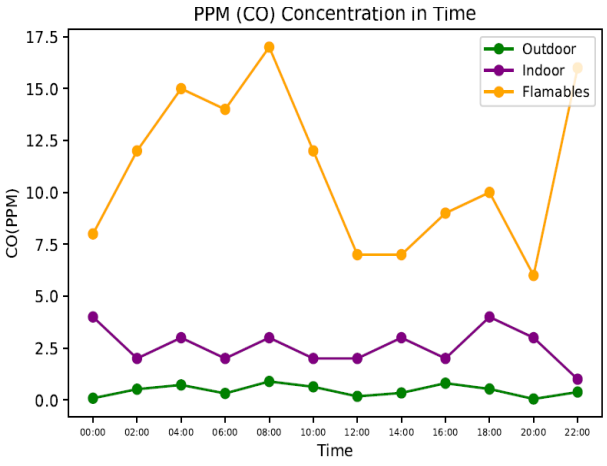

Figure 06: The result of Carbon monoxide (CO) Monitoring system

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

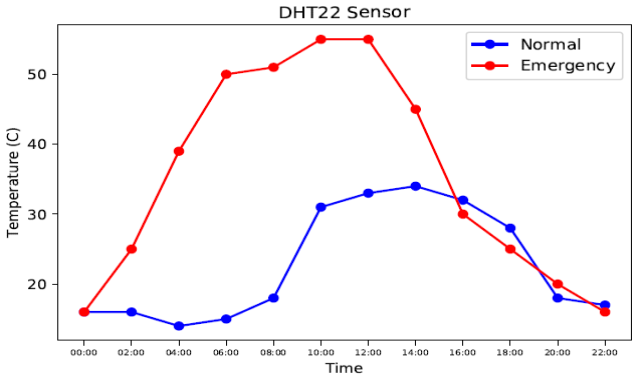

Figure 07: The result of Temperature Monitoring system using DHT22

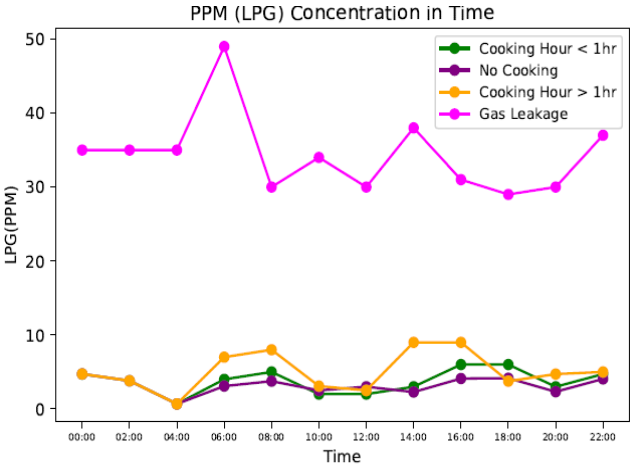

Figure 08: The result of LPG Monitoring system in different condition

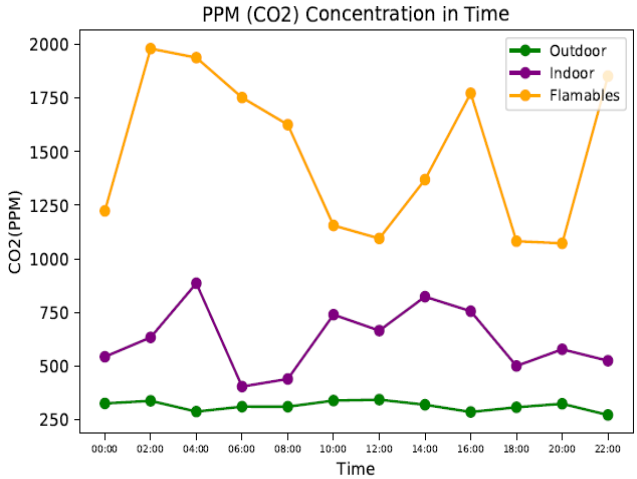

Figure 09: The result of Carbon dioxide (CO2) Monitoring system

In Fig.06, Fig.07, Fig.08 and Fig.09 show the different gas level in three scenarios. As we have implemented in a different scenario to understand the gas variation level. In a smart kitchen environment monitoring of the gas like LPG is very much important along with the others gas. In this work, we try to create the environment and monitor the gas in a different situation and shown in the graph. In an IoT based application, the users can monitor the gas level regularly to avoid any dangerous situation like a fire. In the design, we have explained that all the sensors nodes can be connected to the intermediate fog node for processing it also stores data up to 4hours in its local storage. Fog node is used to processing the information and it will send the information to the users. Finally, the data are sent to the cloud for future reference. In this whole process, security is maintained using ECC techniques. All the sensors node and users are also authenticated to the system before deployed or be part of the system.

VII. CONCLUSION

.In this paper, the authors initially described a framework for smart environment monitoring system. The architecture is based on the Internet of Things (IoT) enabling technology. The basic architecture is a three-layer having fog as a middle layer for computing the collected data from a smart environment. The fog computing supports to the IoT based application are briefly explained with its features. Then the paper proposed a fog-based architecture for a smart monitoring system. The architecture consists of sensor node, fog node, and cloud storage. The proposed framework is tested using the smart kitchen environment having temperature and some gas sensors deployed. The fog node performs the computation in a distributed and cooperative way in a secure environment. We have developed a GUI for user to login to the system and access the data from the sensors. Once registered to the system the user can monitor the collected data. The experimental results show that the proposed framework is well suited to monitor the smart environment in real-time. Once the computation is done by the fog node any deviation found after analysis can be informed to the corresponding authority via a mobile phone. The data visualization part explained the details notification. As per the experimental testbed and results analysis, the proposed framework work perfectly for real-time monitoring of the smart system.

In the future, the authors would like to extend this using Blockchain technology to enhance and improve trust among different fog nodes. As Blockchain is secure and transparent most importantly the transaction is recorded in a digital ledger and every node has that digital ledger database.

REFERENCES

1. Evans D. The internet of things: How the next evolution of the internet is changing everything. CISCO white paper. 2011;1(2011):1.
2. Parthasarathy P, Vivekanandan S. A typical iot architecture-based regular monitoring of arthritis disease using time wrapping algorithm. International Journal of Computers and
3. Applications. 2018;:1.
4. Cai G, Zhao J, Song Q, et al. System architecture of a train sensor network for automatic train safety monitoring. Computers & Industrial Engineering. 2018;.
5. [4] Haghi M, Thurow K, Stoll N. A multi-layer multi-sensor wearable device for physical and chemical environmental parameters monitoring (co & no 2). In: 2017 International Conference on Information and Digital Technologies (IDT); IEEE; 2017. p. 137{141.
6. Keshamoni K, Hemanth S. Smart gas level monitoring, booking & gas leakage detector over iot. In: 2017 IEEE 7th International Advance Computing Conference (IACC); IEEE;2017. p. 330{332.
7. Corbellini S, Di Francia E, Grassini S, et al. Cloud based sensor network for environmental monitoring. Measurement. 2018;118:354{361.

8. Dong S, Duan S, Yang Q, et al. Mems-based smart gas metering for internet of things. IEEE Internet of Things Journal. 2017;4(5):1296{1303.
9. Shi W, Cao J, Zhang Q, et al. Edge computing: Vision and challenges. IEEE Internet of Things Journal. 2016;3(5):637{646.
10. Roman R, Lopez J, Mambo M. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems. 2018;78:680{698.
11. Ni J, Zhang K, Lin X, et al. Securing fog computing for internet of things applications:Challenges and solutions. IEEE Communications Surveys & Tutorials. 2018;20(1):601{628.
12. Bamodu O, Xia L, Tang L. An indoor environment monitoring system using low-cost sensor network. Energy Procedia. 2017;141:660{666.
13. Ayyildiz C, Erdem HE, Dirikgil T, et al. Structure health monitoring using wireless sensor networks on structural elements. Ad Hoc Networks. 2019;82:68{76.
14. Pule M, Yahya A, Chuma J. Wireless sensor networks: A survey on monitoring water quality. Journal of Applied Research and Technology. 2017;15(6):562{570.
15. Malik H, Szwilski A. Towards monitoring the water quality using hierarchal routing protocol for wireless sensor networks. Procedia Computer Science. 2016;98:140{147.
16. Huang Y, Wang L, Hou Y, et al. A prototype iot based wireless sensor network for tra_cinformation monitoring. International Journal of Pavement Research and Technology. 2018;11(2):146{152.
17. Georgieva T, Paskova N, Gaazi B, et al. Design of wireless sensor network for monitoring of soil quality parameters. Agriculture and Agricultural Science Procedia. 2016;10:431{ 437.
18. Wang J, Zhang Z, Li B, et al. An enhanced fall detection system for elderly person monitoring using consumer home networks. IEEE transactions on consumer electronics.2014;60(1):23{29.
19. Lambrou TP, Anastasiou CC, Panayiotou CG, et al. A low-cost sensor network for real-time monitoring and contamination detection in drinking water distribution systems.IEEE sensors journal. 2014;14(8):2765{2772.
20. Liao Y, Mollineaux M, Hsu R, et al. Snowfort: An open source wireless sensor network for data analytics in infrastructure and environmental monitoring. IEEE Sensors Journal. 2014;14(12):4253{4263.
21. Adamo F, Attivissimo F, Carducci CGC, et al. A smart sensor network for sea water quality monitoring. IEEE Sensors Journal. 2015;15(5):2514{2522.
22. Wang K, Gao H, Xu X, et al. An energy-e_cient reliable data transmission scheme for complex environmental monitoring in underwater acoustic sensor networks. IEEE Sensors Journal. 2016;16(11):4051{4062.
23. Wannenburg J, Malekian R. Body sensor network for mobile health monitoring, a diag-nosis and anticipating system. IEEE Sensors Journal. 2015;15(12):6839{6852.
24. Spachos P, Hatzinakos D. Real-time indoor carbon dioxide monitoring through cognitive wireless sensor networks. IEEE sensors journal. 2016;16(2):506{514.
25. Shu L, Mukherjee M, Xu X, et al. A survey on gas leakage source detection and boundary tracking with wireless sensor networks. IEEE Access. 2016;4:1700{1715.
26. Wang H, Fapojuwo AO, Davies RJ. A wireless sensor network for feedlot animal health monitoring. IEEE sensors journal. 2016;16(16):6433{6446.
27. Bonomi F, Milito R, Zhu J, et al. Fog computing and its role in the internet of things. In:Proceedings of the _rst edition of the MCC workshop on Mobile cloud computing; ACM;2012. p. 13{16.
28. Abedin SF, Alam MGR, Tran NH, et al. A fog based system model for cooperative iot node pairing using matching theory. In: 2015 17th Asia-Paci_c Network Operations and
29. Management Symposium (APNOMS); IEEE; 2015. p. 309{314.
30. Oueis J, Strinati EC, Sardellitti S, et al. Small cell clustering for e_cient distributed fog computing: A multi-user case. In: 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall); IEEE; 2015. p. 1{5.
31. Nishio T, Shinkuma R, Takahashi T, et al. Service-oriented heterogeneous resource sharing for optimizing service latency in mobile cloud. In: Proceedings of the _rst international workshop on Mobile cloud computing & networking; ACM; 2013. p. 19{26.

AUTHORS PROFILE

Bhabendu Kumar Mohanta received his B.Tech. degree in Information Technology from V.S.S. University of Technology in 2007 and his M.Tech degree from College of Engineering and Technology, Bhubaneswar in 2012. Presently he is pursuing Ph. D. in International Institute of Information Technology (IIIT) Bhubaneshwar.His research focuses are Information Security and IoT Security and Blockchain Technology. He is also an IEEE student member.

Debasish Jena received his B Tech degree in Computer Science and Engineering, his Management Degree and his M.Tech Degree in 1991, 1997 and 2002 respectively. He got his Ph.D degree from NIT Rourkela in 2010. He is currently working as Associate Professor in IIIT Bhubaneshwar. In addition to his responsibility, he was also IT, Consultant to Health Society, Govt. of Orissa for a period of 2 years from 2004 to 2006. His research areas of interest are Information Security, Cloud Security, IoT Security and Blockchain. His professional memberships include IEEE, ACM, ISTE, IACSIT, MIE (I), CSI, and OITS.