International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

EVMS: Explosive Vehicle Monitoring System with IoT

Brahmaji Godi, Appala Srinuvasu Muttipti, V. Sangeeta, N. Renugadevi

Abstract*: Internet of Things (IoT) is playing a dynamic role in day to day human lives. It is an integrated platform relates with physical sensor components, wireless device networks, cloud based databases and application monitoring systems. Technology of IoT expanded in many research areas such Agricultural forming, Air pollution, Wastage management, E-health monitoring etc. In this scenario the proposed system which relates to logistical industrial operation so, the authors try to use the Internet of Things as a solution to the problem. At present moving explosive vehicles are not monitored specifically by any online automated system. The aspect of monitoring and controlling moving heavy explosive vehicles is tough, which are carrying huge amount of cargo such as pharmacy chemicals, oils, gases. It is very difficult to monitor the moving vehicles in industrial areas and other locations. The major problem is with the identification of certain issues such as local and global positioning, parking places, filling stations road and traffic directions, sound identification, leakage management, and other safety measures of the vehicles. The primary elements of the proposed IoT system are analyzed based on IoT architectural model and wireless sensor networks. It supports the physical devices to work connectively as to collect and send the exact information through the online application to monitor the moving explosive vehicles. This system is further called the Explosive Vehicle Monitoring Systems (EVMS). The authors believe that the EVMS can regulate all major problems mentioned above. This paper will observe the possibilities of future implementation of the EVMS system.

Keywords*: Internet of things (IoT), Device sensors, Cloud storage, Explosive vehicle monitoring system (EVMS).

I. INTRODUCTION

IoT is a newly emerging technology in real-world connecting sensor based devices to the internet from which data can be accessed. The process is done by using sensors, actuators, and transducers and is monitored by the IoT automation systems. When the sensor devices are connected to the internet, they behave heterogeneously in accessing network throughout ubiquitous accessibility and connectivity of network devices. In the physical layer, the sensor will work with physical devices or sensor nodes that provide the information by sensing the exact information of real-time environment and collecting information as well as data adaption can also be handled. In the next part, an actuator can generate the energy into motion, so actuators are used whenever there is need to switch on/off another devices or equipment by applying a force route to control it, where a decision is made and a corresponding command is sent back to an actuator in respond. Example: Temperature sensor reads the temperature in a room and gives the message to the actuator and it checks condition statement, thereafter it instructs the nearby air conditioner to switch on/off. As well as Transducers can also convert one form of energy into another form, for example, Loudspeakers are designed using a simple transformations energy using electro sound transducers which transform an electrical acoustic signal into sound. It can be observed in the fig1.

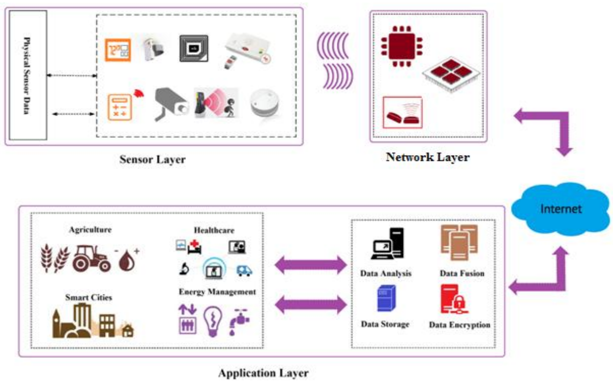

Fig.1 Basic IoT Architecture layers

The second step network layer is connected with gateways along with various software and hardware is used as nodes of gateways such as computer, modem, router, servers, and proxy servers, etc. The primary devices are used in network gateways although middleware network is supporting protocol to handle communication between the node devices, servers, and cloud databases. Here, some of the wireless sensor networks are used in communications such as Radio Frequency Identification (RFID), WiFi protocols, Zigbee protocols, 6LowPAN, RPL, Nearfield communication (NFC), and HART which are some of the important procedure used in IoT network communication.

The third step is the application layer supported to lower layers, where the cloud database provides efficient and related services such as dynamic management, sharing resources, reliability, and scalability involved in service provision.

Manuscript published on 30 September 2019
* Correspondence Author

Brahmaji Godi*, Department of Computer Science and Engineering, Raghu Institute of Technology, Visakhapatnam, India. Email: brahmajigodi@gmail.com

Dr. Appala Srinuvasu Muttipati, Department of Computer Science and Engineering, Raghu Institute of Technology, Visakhapatnam, India. Email: srinuvasu.mutti@gmail.com

Dr. V. Sangeeta, Department of Computer Science and Engineering, Raghu Institute of Technology, Visakhapatnam, India. Email: sangeetaviswanadham@yahoo.com

Dr. N. Renugadevi, Department of Computer Science and Engineering at National Institute of Technology Warangal, Telangana, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

Cloud offers maximum IoT application resource, edge computing, data analytics, data preprocessing, data storage, mixed data analysis send through proper data encryption standards securities in end to end device services.

Finally, the usability and scalability IoT is expanding drastically in IoT architectural system which helps to design and implement systems such as smart home applications, buildings automation, agricultural, vehicle monitoring, industries and some more systems which covenants in real-time application.

The scope of the IoT is currently increasing day-to-day in the industrial sector improving the safety measurements, wastage management, security, health and medical etc. The proposed system is designed for industry issues and making tasks much efficient and effective. The usages of the industrial IoT is going to enhance the economic and financial phase of the business world. The industries are always looking for business growth in many areas where IoT maps the industrial requirement and tries to harmonize both technology and business development. It helps the growth in many factors in areas of production, manufacturing, transportation, logistics, utilities, smart energy consumption, and many others areas.

II. RELATED WORK

Y. Benazzouz et. al. [1] described IoT devices playing key role in cloud-based architecture. The cloud environment model creates virtual execution environment of decentralized nature for resources and services expanded through cloud platform. A cloud grants secure access shared resources by all the device models. It represents data abstraction of IoT devices accessed through gateway connected to Application Program Interface (API) to cloud services. It also provides business properties of application developer's inadequate new business model.

R. Brunnader et. al. [2] described novel intelligent vehicle monitoring systems have been classified into three main modules Video Information System (digital camera), Environment Information System (temperature, humidity) Position Information System (Position). Here all these transducer gathers data in electronic datasheets which are utilized to classify the kind of operation conceded in wireless sensors, actuators, and transducers can send the data through secure network communications. The basic model IEEE 1451.2 standard transmits data request to monitor the systems, the projected architecture might deliver unified access through numerous wireless sensors and actuators with high performance of devices meeting the real-time necessities. It is implemented through System on chip (SoC) and Field programmable gate array (FPGA) chips Technologies which work with less hardware and with low power battery consumption is used to design and maintenance of vehicle monitoring systems.

S. Wang et. al. [3] discussed routing architecture with Autonomous Systems of Things (ASoT), connecting with the sensors and Radio frequency identification (RFID) tags used for smart electromechanical devices surrounded in network. Local communication systems with IoT 6A is connected to International Telecommunication Union (ITU) and Cluster of European Research Projects on the Internet of Things (CERP-IoT) which work with a notation of any time, anything, and any service. ASoT configure with inside and outside networks with other conglomeration of autonomous system runs with Interior gateway protocols (IGP), Routing information protocol (RIP), open shortest path first (OSPF), Intermediate System-to-Intermediate System (IS-IS), Exterior Gateway Protocols, Border-Gateway protocols these routing algorithms are proposed for highly various networking environment and advanced applications, these autonomous systems brings new scope of challenges on inter-domain network systems.

S. Park et. al. [4] described on water leakage system monitoring the data using printed circuit board (PCB) data from remote sensor of different types (acoustic, pressure, temperature, flow rate, sound, vibration etc) collected and monitoring using IEEE 802.15.4 wireless sensor network work with sensor, antenna, data transmission, network protocols application and its functionality. Bit cloud provides a software development plot form for reliable, scalable and secure wireless network PCB configured will operate as network coordinator router or end devices, wireless sensors network monitoring system (WSNM) contain the information of node history and node parameters, using WSNM monitor systems mostly implemented in industries, agriculture, and military services.

N. Vidgren et. al. [5] discusses security threats in Zigbee empowered systems. The primary attack is to disrupt the Zigbee end devices by sending a superior signal so that the attacker may masquerade or extract the data available in the Zigbee end devices. The attack will continue until the battery runs out completely. The succeeding attack is manipulating the key interchange process through ZigBee protocol utilizing a typical security level which is implemented in wireless personal area network and Radio Frequency communication. It is stress-free to the usage of wired or infrared communication then it also makes eave dropping tranquil. Here disturb Jam wireless, ZigBee network is very large scalable in multiplexing, enhancing the securities feature in IEEE.802.15.4.2003 and also simplified in IEEE.802.15.4.2006 standards. Involvement of ZigBee protocol security levels are supported at trusted centers, secured authentication, secured encryption, secure data integrity and newness of data; using cipher block chaining technique and message authentication coding which can prevent DoS attacks.

III. PROPOSED MODEL

Explosive vehicle monitoring system (EVMS) is supported by a global positioning tracking system and various sensors are added to handle multipurpose ideal solution to regulate the current system. The proposed model describes the EVMS which consists of various sensors, actuators, and transducers that can handle data enrichment, data gathering, and data collection by using intelligent nodes.

Retrieval Number: C6546098319/2019©BEIESP
DOI:10.35940/ijrte.C6546.098319
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
Sciences Publication

Microcontroller collects data from the sensor devices and sends the data through a gateway using wireless sensor networks to its nearby antenna or signaling station. In the next level, the data is updated or stored in the cloud database. Here, we have chosen a cloud database platform which is mainly a multi-stored sharing environment providing to store the very large scale information.

An application Programming Interface (API) acts as a medium layer which creates a connection establishment between cloud database storage and EVMS applications. Here cloud storage show a dynamic role in the collection of distributed data through secured authenticated channels and authorized endpoints as shown in fig 2.

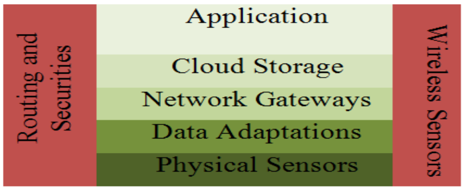

Fig. 2 IoT Architecture layer for EVMS

Cloud data storage provides high quality of service (QoS), efficient resource provider along with heuristic algorithms that are implemented in data storage, data adaption, data analytics and encryption [6]. EVMS control monitoring system has several features such as; periodical observation, providing visualized statistical data, keeping track of on-road vehicle condition and position and message alerts to the mobile admin. EVMS network architecture connects cloud database application to API. As a result, the data can be accessible to desktops, laptops, or any mobile terminals. The admin will regulate and suggest appropriate actions to the vehicle in-charge. Fig 3 describes the proposed model of EVMS architecture.

Fig. 3 Propose model for EVMS

Further classification of monitoring systems can handle issues like filling and leakage identification, road monitoring and identification of surrounding vehicles, other object detection, safety measurement and global positions of an explosive vehicle in detail [7-8]. Firstly the vehicle connected to an on-board computer. Primary element of the vehicle is fuel level indication check-ups, using fuel level indicators it can justify traveling distance to reach the destination. Consequently, with this it can reduce the consumption of vehicle operating cost and economize the transportation. It also assists in timely decision making in many other factors based on received relevant data from the vehicle and progresses the overall competence of the business process. Secondly, the Global Positioning System (GPS) based on a vehicle monitoring system that allows simply tracking the position and location of vehicles in a real-time environment. The vehicle consists of a GPS with related software that is fixed in it, through that data will be collected geographically and later send to EVMS applications where data can be visualized in the form of pictures on the console. The GPS device can also send physical data alerts about the vehicle's disorder and definite events which are usually sensible through the GPS device. For illustration, one of the utmost generally traced events is door locking (open/closed), ignition (on/off), vehicle's speed automation and so on.

EVSM is regulated with a sensor automated system which consists of two major classifications mainly Road monitoring and Container monitoring. Here the whole vehicle is monitored and controlled with various sensors collecting the data at different parts of the vehicle such as Filling and leakage, pressure, road monitoring system which consists of four main sensors such as Accelerometer force sensor, Ultrasonic sensor, Motion and Camera sensor, GPS sensors, Container monitoring system which consists of Gas detection sensor, Pressure sensor, liquid Filling sensor and the Flow sensor [9]. The classification of sensors used in the proposed system is depicted in fig 4.

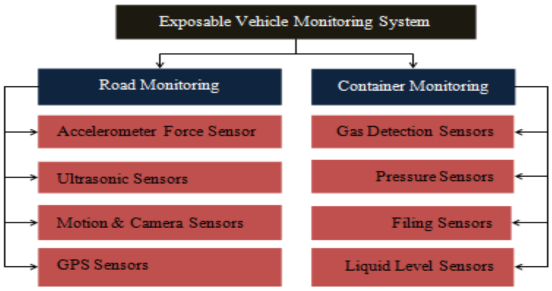

Fig. 4 EVMS work flow chart

IV. ANALYSIS

By considering the EVMS we have classified the various sensor behaviors through synthesized analyses [10] as follows,

- First level of analysis: Accelerometer sensor which checks and regulates the speed of the vehicle based upon the two factors: distance travel and speed limit if the driver exceeds speed/distance limit, accelerometer sensor check the reading of the vehicle and gives an alert message through (EVMS) along the wireless signal is generated to led bulb will be indicated to the driver to control the speed.
- Second level of analysis: Ultrasonic sensor detects the movement of targets and measure the distances of other vehicles. Along with this, the sensor can identify the movement of the object and convert the received analog signal into the digital form to monitor the system.
- Third level of analysis: Motion and Camera sensors can identify the theft when vehicles are at parking. Even in light fall and night they can detect the movement of an object and immediately switch ON the light and gives active information to the monitoring system to regulate locking systems of containers.

Retrieval Number: C6546098319/2019©BEIESP
DOI:10.35940/ijrte.C6546.098319
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering & Sciences Publication

- Fourth level of analysis: Global position system sensor is used to track the vehicle position and provides the best shortest path which is suitable to the explosive vehicle and also provides critical suggestion using satellite-based augmentation systems for future enhancements.
- Fifth level of analysis: Gas detection sensor checks humidity and contamination level in the container and detects leakage levels with remote access control and generates low-level message alert to EVMC along with low-level wireless signal is sent to red light indication to the driver.
- Sixth level of analysis: Pressure sensor is used for the measurement of Gases and Liquids. Usually, these sensors act as transducers used in the gas-liquid sensor, digital pressure sensor, hydraulic pressure sensor, pressure transducer used for oil, fuel, gas, etc.
- Seventh level of analysis: Filling level sensor or flow sensor identifies the fluid flow in fuel tanker for instance if the maximum flow is 90% of filling level but the current fuel level is 30% then sensor checks min-max filling liquid level in the container and gives the signal to indicate whether low level, full level or empty.
- Eight levels of analysis: Liquid level sensor is used to detect and identify some types of an irresistible liquid floating which rises and falls in the container, switch option is used to control and indicate by an alarm or continuous vibrations as the liquid reaches the limit. The structural designs of the vehicle with sensors are shown in fig 5.
-

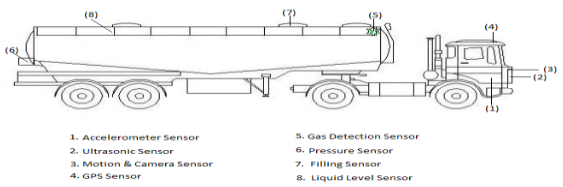

Fig. 5 Classification of Sensors on Explosive vehicle monitoring system

V. CONCLUSION

The proposed architecture system EVMS fulfils the real-time requirements of industries. Using the Internet of Things for explosive vehicles can easily monitored through EVMS in various wastage management, GPS and vehicle navigations, environment protection, and public security at both industrial and non-industrial locations. Hence this EVM system can regulate and control the drawbacks of an existing explosive vehicle. Thereby EMVS can handle bio-environment factors in eradicating major leakage detection, accidents, exposures of oil, gases, chemicals, etc. In this scenario, most of the business operations which are related to transportation and logistics can reduce the risk. Finally, EVMS plays a vital role in facing new challenges in automating systems for the development of industrial operations.

REFERENCES

1. Y. Benazzouz, C. Munilla, O. Günalp, M. Gallissot and L. Gürgen, "Sharing user IoT devices in the cloud," 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, 2014, pp. 373-374.
2. M. A. Khan and S. Ojha, "Virtual Route Tracking in ZigBee (IEEE 802.15.4) enabled RFID interrogator mesh network," 2008 International Symposium on Information Technology, Kuala Lumpur, 2008, pp. 1-7.
3. S. Wang, Y. Hou, F. Gao and X. Ji, "A novel IoT access architecture for vehicle monitoring system," 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, 2016, pp. 639-642.
4. S. Park, N. Crespi, H. Park and S. Kim, "IoT routing architecture with autonomous systems of things," 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, 2014, pp. 442-445.
5. N. Vidgren, K. Haataja, J. L. Patiño-Andres, J. J. Ramírez-Sanchis and P. Toivanen, "Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned," 2013 46th Hawaii International Conference on System Sciences, Wailea, Maui, HI, 2013, pp. 5132-5138.
6. R. Biswas and R. Giaffreda, "IoT and cloud convergence: Opportunities and challenges," 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, 2014, pp. 375-376.
7. M. A. Ikram, M. D. Alshehri and F. K. Hussain, "Architecture of an IoT-based system for football supervision (IoT Football)," 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, 2015, pp. 69-74.
8. Miladinovic and S. Schefer-Wenzl, "NFV enabled IoT architecture for an operating room environment," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 98-102.
9. R. Brunnader and G. Holler, "Experimental validation of a leakage and fill-level estimation method for vented tanks," 2011 Fifth International Conference on Sensing Technology, Palmerston North, 2011, pp. 395-398.
10. K. K. Kishore , G. Brahmaji, D. Manivannam and A. S. Muttipati, “Role of IoT in Enhancing Agricultural Techniques”, International Journal of Innovative Technology and Exploring Engineering, Vol. 8(7),2019, pp.332-334.

AUTHORS PROFILE

Mr. Brahmaji Godi MSc.IS from Andhra Univerisity in 2003,M.Tech CST from Andhra University in 2009, Visakhapatnam .Currently working as Assistant Professor in Department of Computer Science and Engineering at Raghu Institute of Technology Visakhapatnam. He had published few papers in various reputed journals and he is a valid member at IAENG, SDIWC. His main research work focuses on Internet of Things, Cloud computing and Wireless networks.

Dr. Appala Srinuvasu Muttipati currently functioning as Associate Professor in the Department of Computer Science and Engineering at Raghu Institute of Technology, Visakhapatnam. He had awarded Ph.D. in 2018 and M. Tech in 2011 from GITAM University and Master of Computer Application in 2008 from Andhra University. He had 10 years of teaching experience. He had published 8 research papers from reputed International Journals. He is a member in IEI and professional member at IFERP. His main research work focuses on Data Mining, Big Data, Machine Learning, Cloud Computing and Internet of Things.

Dr. V Sangeeta currently working as professor and Head of the Computer Science and Engineering Department at Raghu Institute of Technology. She had awarded Ph.D in the year 2016, M.Tech in the year 2006, Master of Computer Application in the year 1997 from Andhra University. She had 21 years of teaching Experience and published more than 10 journals. She is a valid member in ACM and her Research areas from Data Mining, Computer Networks and network securities.

Dr. N. Renugadevi is currently serving as an Assistant Professor in the Department of Computer Science and Engineering at National Institute of Technology Warangal, Telangana, India. She received Ph.D from National Institute of Technology, Tiruchirappalli, Tamil Nadu in 2017. She is carrying an experience of 13 years in the teaching profession. Her research interests include Cognitive radio wireless networks, Group key management techniques and Secure group communication. She is a member of IEEE and life member of ISTE.