ISSN No:-2456-2165

Economical Visitor's Identity Provider

Dr.D.Sivakumar[1],M. prem Anand[2],H.K.Ajith Kumar[3] ,R.Ajith Kumar[4],V.Gayathri[5]
[1]Professor,Department of Electronics and Communication Engineering, Easwari Engineering College
[2] Asst.Professor,Department of Electronics and Communication Engineering, Easwari Engineering College
[3,4,5]Bachelor of Engineering Student, Department of Electronics and Communication Engineering,Easwari Engineering College

Abstract:- The growth of the internet era has paved way for development of numerous applications. IoT plays a vital role in designing the devices that are very helpful to people by just a click away from the services they want to use. All the devices connected together by making use of internet connection and working for the same objective is termed to form an IoT environment. IoT plays a vital role in industrial applications especially in securing the industry from internal and external threats. Security is a prime aspect that needs to be looked into for any kind of application. Many researchers are currently working on various security aspects for various domains. In this paper, we have proposed a secure and efficient model for monitoring industries based on the IoT based environment. In this paper, the model is developed for monitoring the people walking in and out of an industry or a company. This is done by making use of the beacon ID tracking system. The proposed approach is evaluated and the performance of the approach is observed to be better than any other traditional nutrition monitoring system.

Keywords:- *IoT, Beacon ID, Tracking System, Monitoring, Secure, Efficient, Log, Application Processing*.

I. INTRODUCTION

IoT is one of the emerging technologies that is used widely in many fields. Some of them are Smart homes [1], Smart classrooms [2], Health Care [3] and lots more. IoT is responsible for communicating with numerous devices when connected to the internet [4]. Security plays an important role in all applications. There are many threats that are endangered when the devices are connected to the internet. Numerous data are being exchanged from one device to another and this makes it a repository where a huge amount of data gets stored. Many hackers are in need of these data and break all the security issues that are available in protecting the data. Though the system is secured in all the aspects there always exists a way to break it.

Security is a critical aspect that needs to be considered while using all possible applications. One such is in the use of industries. There are numerous people who way in and out in an industry or a company. It is not mandatory that all these people would be having their identity proof. Giving off temporary identity proofs is advisable but is not secured as it seems to be. In this case, there occurs a need to examining the security of the industry. In this paper, we have proposed a model for securing the industry by perfectly monitoring the people who are entering and exiting the company or the industry. This is done by making use of the Beacons. A beacon is a device that emits signals instead of light. These devices are usually connected to the Bluetooth of the Smartphone's and are used to monitor the entire IoT environment. The efficiency of the model is evaluated using various performance evaluation parameters and is observed to work efficiently when compared to the existing systems. The rest of the section is as follows: Section II deals with Literature Survey needed for the work, section III consists of the technical frame implemented in the work and section IV consists of obtained experimental results. The paper is concluded by mentioning the relevant future scope that could be added to the proposed work.

II. RELATED WORK

Numerous applications have been developed by using beacons to secure the systems in an IoT environment. some of the research works that make use of beacons are stated. KK Venkatasubramanian [5] designed a secured health monitoring system for sensor applications that was intended to design secure the health care system. In this approach beacons device was used for transmitting and receiving the messages from the nodes. Mukherjee.S has designed a patient health management system. The architecture comprises of nodes that are used for communicating with the patients and the hospital staffs [6]. In case of an emergency, the patient or the family members could easily be communicated with each other and make them realize the situation better and in a fast way. In [7], the author has proposed a mechanism for securing vehicles by analyzing various vehicular behaviors. The security is provided through beacons where each vehicle using it is able to know its environment and other details. This could be used for knowing if the vehicle can go in a particular route or not and if any other alternate route is resent for it. P.Papadimitratos [8], has also made use of beacons in vehicular security. Each vehicle transmits a message every 10minutes and rest of all the other vehicles connected to the systems is able to receive the transmitted message from the sender-beacon. Kolavenu [9] has proposed a method by combining the RF technology with the beacon nodes for locating and tracking the people. It is proposed to lower the squared error between the position estimate and is completely based on the signal strength. In [10], the research work has a proposed system for locating and tracking the devices that are available in the environment where it is been deployed. Bluetooth Low Energy is widely used many applications for transmitting the messages.

Bluetooth plays a vital role in the exchange of messages when a beacon is used. Liu *et al.* [11] proposed a model which is used in latency conditions for device recovery in Bluetooth. Later, the authors performed vast

ISSN No:-2456-2165

energy measurement techniques for the tracking of BLE devices in Bluetooth but interference is not considered. Chong *et al.* [12] developed a model for measurement of throughput and energy consumption in ZigBee Network using Bluetooth Classic interference.Stranne*et al.* [13] performed experiments to develop model on mutual interference on the throughput of Bluetooth classic [14]. Howitt [15] developed a model for interference between independent Bluetooth connections and considered one interferer. Goldenbaum*et al.* [16] designed a model that consists of multi-antenna sensor networks with interference has no claim of performing any experiments. Gomez *et al.* [17] considered BLE throughput based on the bit error rate. The model is verified using simulation. Kindt*et al.* [18] designed a very extensive energy model consisting of BLE and verified it using an experiment. Even in this system, the interference was not taken into account.

III. SECURED AND EFFICIENT MONITORING SYSTEM

In this paper, we have proposed a work that consists of developing an environment where the monitoring of the people is done. There are many companies and industries where numerous people enter and exit on a daily basis. All the people coming inside the industry need not be a staff of the industry. There will be numerous people who would be entering it for other purposes also. Providing a temporary identity card for them is an alternate way of securing the system but it is not the ideal way now due to increase in the technical issues. In order to make the system more effective by securing it the use of Beacon nodes are used. The beacon nodes are present in the IoT based environment and it can access the people who are not actually authenticated. These nodes are connected to the smartphones for providing an alert when a new unauthorized entry is made into the system. The beacon nodes are used for transmitting the signals and to make it more secure alert messages are sent to the admin which can actually look into who have accessed the system without proper authentication. In the existing system, most of the beacon nodes are actually used for tracing the people in during commuting in public transportation. The same idea is implemented here but in an industry environment. It is not always possible to show the original ID proof to the company staffs and is not recommended to handover the originals of the visiting people to the security guards. By making use of this beacon ID we design an application for the office. Whenever the person visits the office, he has to enter the details of the application. While entering the office for the next time, the person has to switch on the beacon node in his smartphones. The details are automatically sent to the server. In this case, all the details of the user while inside the office continuously save in the server. The in-time, the out time, the places where he has gone while in the office timings and lots more. This makes it easier for monitoring the staffs when a huge amount of them are present and we want to monitor them while sitting in one place.

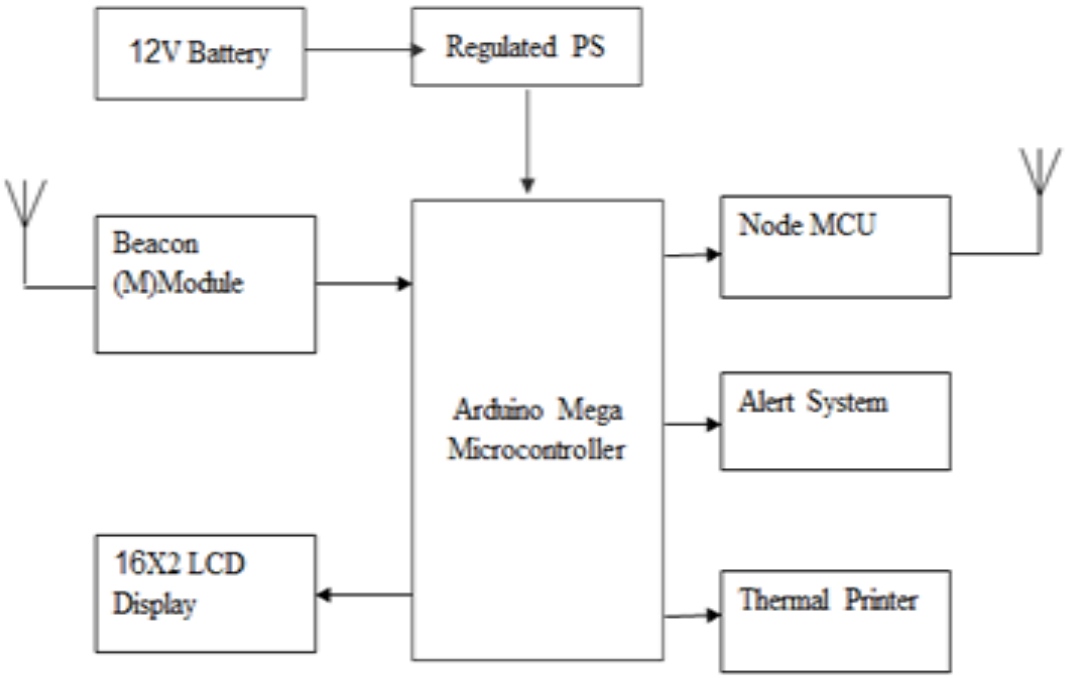

Fig 1:- Block Diagram of Transmitter of Secured Monitoring System

Fig. 1 shows the receiver unit of the beacon module. It is connected with the microcontroller and is given a supply of 12V. The display is connected so that the status of the node can be displayed. The microcontroller to which the beacon module is connected is in turn connected with the printer and the alert system.The printer is used to print the details of any registered user and the alert system is used to alert the admin in case of any unauthorized access inside the industry. Fig 2. shows the transmitter unit of the module where the beacon unit is connected to the power supply for continuously monitoring the environment.

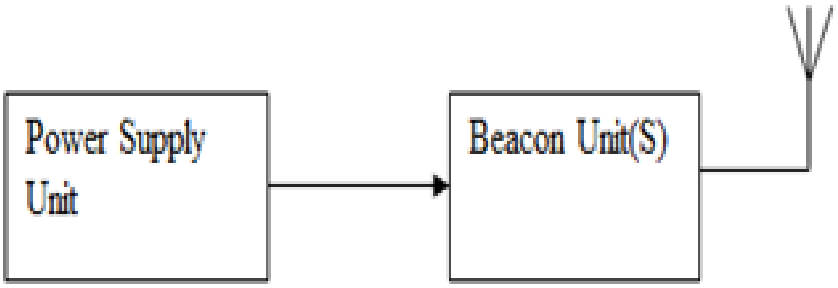

Fig 2:- Block Diagram of Transmitter of Secured Monitoring System

IV. EXPERIMENTAL RESULTS

The system was evaluated on a real-time basis. Numerous information about the users were asked to log in. The user was made to enter all his personal information like his name, gender, his designation and all the other requirements like his Aadhar number, PAN number and lots more The efficiency of the application was done on various parameters.

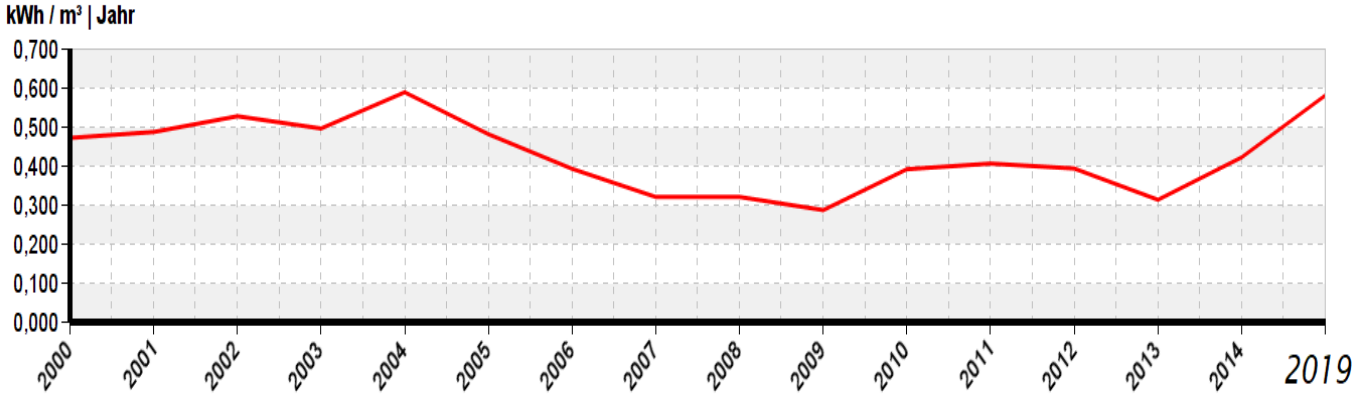

Fig 3:- The efficiency of the Monitoring System

Some of the parameters involved the speed, computational time, the fault tolerance and the loss of packets y computing the miss and the hit rates of the signal transmission. Fig. 3 and 4 shows the transmission speed and efficiency of the proposed model when used in an IoT based environment.

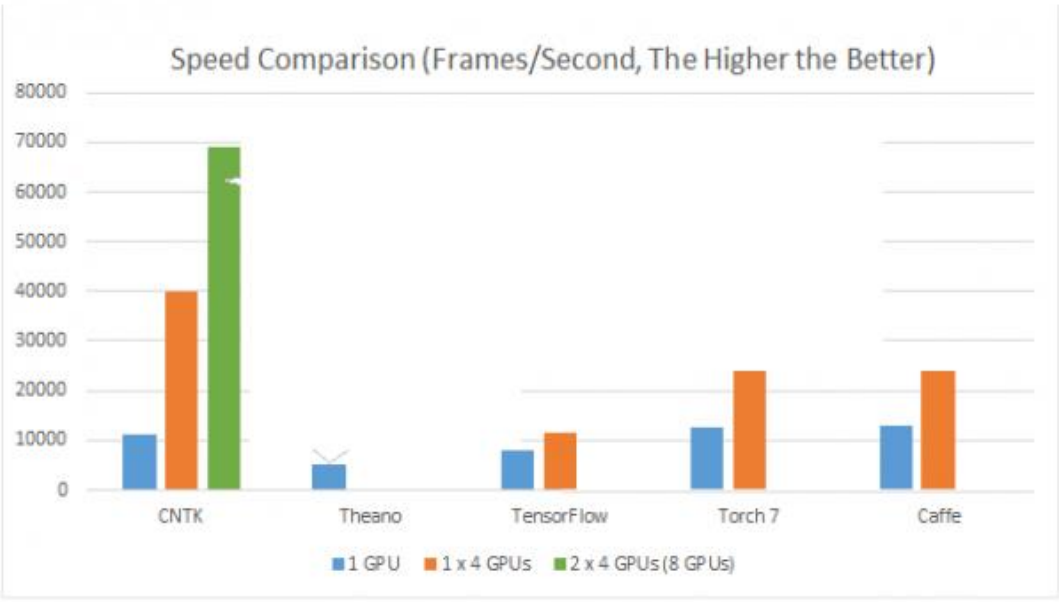

Fig 4:- The Efficiency of the Monitoring System

ISSN No:-2456-2165

V. CONCLUSION

Monitoring is a vital aspect that needs to be done in any industry and company. Proposer functioning of the entire system happens only when there is a perfect monitoring system. While taking the importance of monitoring in an environment, we have proposed a model for monitoring the industrial environment by using beacon ID. The proposed model is served to be efficient and secured when used in an IoT based environment where several other devices are connected to the system and it will be used in national and international trade fairs. The movements of the people inside the industry are well monitored and are observed to be effective when compared to the previous other existing systems. The performance of the system is evaluated and is plotted. From the observation, it can be concluded that the proposed model monitors effectively when compared to other existing systems. As a future work, the system could be made more secure by using a security protocol to the system and making the information being stored in the system more secure. Outcome of application, it will be using in train ticket providing, so that everyone can enter into railway station and toll gate (for vehicles) after taking tickets by using the payment wallet options.

REFERENCES

[1]. Basiotis, P.P., Welsh, S.O., Cronin, F.J., Kelsay, J.L., Mertz, W., et al.: Number of days of food intake records required to estimate individual and group nutrient intakes with defined confidence. J. Nutr. 117(9), 1638–1641 (1987).

[2]. Darby, A., Strum, M.W., Holmes, E., Gatwood, J.: A review of nutritional tracking mobile applications for diabetes patient use. Diabetes Technol. Therapy. 18(3), 200–212 (2016)

[3]. Fontana, J.M., Sazonov, E.: Detection and characterization of food intake by wearable sensors. In: Wearable Sensors, pp. 591–616 (2014)

[4]. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of Things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. 29(7), 1645–1660 (2013).

[5]. Venkatasubramanian, K. K., & Gupta, S. K. (2006, October). Security for pervasive health monitoring sensor applications. In Intelligent Sensing and Information Processing, 2006. ICISIP 2006. Fourth International Conference on (pp. 197-202). IEEE.

[6]. Mukherjee, S., Dolui, K., &Datta, S. K. (2014, February). Patient health management system using e-health monitoring architecture. In Advance Computing Conference (IACC), 2014 IEEE International (pp. 400-405). IEEE.

[7]. Schmidt, R. K., Leinmüller, T., Schoch, E., Held, A., &Schäfer, G. (2008, June). Vehicle behavior analysis to enhance security in vanets. In Proceedings of the 4th IEEE Vehicle-to-Vehicle Communications Workshop (V2VCOM2008.

[8]. Papadimitratos, P., De La Fortelle, A., Evenssen, K., Brignolo, R., & Cosenza, S. (2009). Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation. IEEE communications magazine, 47(11).

[9]. Kolavennu, S. N., &Huseth, S. D. (2008). U.S. Patent No. 7,420,510. Washington, DC: U.S. Patent and Trademark Office

[10]. Buck, James J., Peter Sackschewsky, Victor Rompa, and Joseph P. Newell. "Beacon Based Tracking Devices and Methods for Using Such." U.S. Patent Application 12/041,746, filed December 25, 2008.

[11]. J. Liu, C. Chen, Y. Ma, and Y. Xu, "Energy analysis of device discovery for bluetooth low energy," in Vehicular Technology Conference (VTC Fall), 2013 IEEE 78th, pp. 1–5, IEEE, 2013.

[12]. W. Chong, H. Y. Hwang, C. Y. Jung, and D. K. Sung, "Analysis of throughput and energy consumption in a zigbee network under the presence of bluetooth interference," in Global Telecommunications Conference, 2007. GLOBECOM'07. IEEE, pp. 4749–4753, IEEE, 2007.

[13]. A. Stranne, O. Edfors, and B.-A. Molin, "Energy-based interference analysis of heterogeneous packet radio networks," Communications, IEEE Transactions on, vol. 54, pp. 1299–1309, July 2006.

[14]. Howitt, "Mutual interference between independent bluetoothpiconets," Vehicular Technology, IEEE Transactions on, vol. 52, no. 3, pp. 708–718, 2003.

[15]. M. Goldenbaum and S. Stanczak, "On multiantenna sensor networks with interference: Energy consumption vs. robustness," in Smart Antennas (WSA), 2012 International ITG Workshop on, pp. 125–132, IEEE, 2012.

[16]. . Gomez, I. Demirkol, and J. Paradells, "Modeling the maximum throughput of bluetooth low energy in an error-prone link," Communications Letters, IEEE, vol. 15, no. 11, pp. 1187–1189, 2011.

[17]. P. Kindt, D. Yunge, R. Diemer, and S. Chakraborty, "Precise energy modeling for the bluetooth low energy protocol," arXiv preprint arXiv:1403.2919, 2014.

[18]. M. Siekkinen, M. Hiienkari, J. Nurminen, and J. Nieminen, "How low energy is bluetooth low energy? comparative measurements with zigbee/802.15.4," in Wireless Communications and Networking Conference Workshops (WCNCW), 2012 IEEE, pp. 232–237, April 2012.