International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

SMART CARD BASED AUTOMATED TOLL PLAZA SYSTEM

MR.SATHISH KUMAR[1], P.DHIVYA[2], R.ABINAYA[3], S.INDHUMATHI[4], T.DEEPIKA[5]

[1]ASST PROFESSOR, DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING, PANIMALAR ENGINEERING COLLEGE, CHENNAI, TAMIL NADU, INDIA.
[2,3,4,5] STUDENT, DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING, PANIMALAR ENGINEERING COLLEGE, CHENNAI, TAMIL NADU, INDIA.

Abstract - – *Internet of things is one of the most emerging and popular technology which has changed our life, by impacting different areas such as shopping, production, storage, monitoring physical devices etc. Internet of Things concept has a possibility to combine different devices from different areas results in exchange of different data types through different networks. The aim of our project is to design a system which automatically identifies an approaching vehicles and record toll gate name, date and time. If the vehicle belongs to the authorized person, it automatically opens the toll gate and a predetermined amount is automatically deducted from its account. This will reduce Traffic congestion at toll plazas and helps in lower fuel consumption. This technology can be used where time and efficiency are the matter of priority in toll collection systems of present day. When the vehicle moves through the toll gate on any road, it is indicated on the RFID reader that it has crossed the clearing. Thus the reader reads the information in the tag and the transaction takes place through a centralized data base and the aftermath details of the transaction is intimated to the user's mobile through GSM technology. The need for manual toll based systems is completely reduced in this method. In the existing system, sensor nodes are equipped with a Global Positioning System module as to provide geo location information of their sensed data. However, GPS modules present additional production costs and are also power consumption. So In this project, we propose, analyze, and experimentally demonstrate a new localization problem found in many large scale WSN deployments: the Wireless Localization Matching Problem. Here the locations of the sensor nodes are known a priori and a deck of m cards labeled 1 through m is shuffled randomly. A match occurs when the number on the card matches the card's position in the deck*

***Key Words*: Internet of Things, IoT, connection, network, programming, performance, vehicle toll payment.**

1. INTRODUCTION

Interfacing different small resource constrained devices through the Internet to centralized or cloud systems results in binding different services and data transfer. Such concept called Internet of Things (IoT) aims to connect different physical environments, implementing different services such as measurement, control, analytics, reporting, etc. Such connectivity based on lightweight Internet protocols is not only constrained to a centralized system, it has the ability to interface other IoT devices together forming big and dynamic network. The IoT can be considered as one type of environment in which all physical objects, peoples and animals are having unique identity and they are able to transfer data over the network without any interaction. IoT is the combination of different technologies; it evolved the internet, wireless technologies and micro-electromechanical systems (MEMS). This terminology can be considered as the Internet of Everything. A thing presents in the IoT environment can be a man-made object, a person with a heart monitor implant, any animal with a biochip transponder and any vehicle with sensor. All these things are assigned with one unique IP address and have the ability to transfer data over the Internet. So far, IoT closely related to Machine-to-Machine (M2M) communication in manufacturing, oil, gas and power industries. The IPv6s having huge addresses space and with help of IPv6 we can assign a unique address to each object present on the surface of earth. IPv6 is a very significant feature for the development of Internet Things.

1.1 EXISTING SYSTEM

There are two methods of collecting tax presently used they are First is the traditional manual method where one person collects money and issues a receipt. In the existing system, sensor nodes are equipped with a Global Positioning System (GPS) module as to provide geo location information of their sensed data. However, GPS modules present additional production costs and are also power hungry to run (about 30mA at 3.3V). Moreover, GPS is not accurate in indoors. The above methods are subject to errors caused by background noise, wireless multipath fading, shadowing, non-line-of-sight (NLoS), path loss, etc. Hence empirical models are often evoked to retune and refine the accuracy of the localization methods. These are sometimes costly and time-consuming since model parameters need to be adjusted for each specific environment. Internet is a worldwide structure of interconnected IP networks that links billions of computers together. Network infrastructure comprises routers, gateways, switches, repeaters.

1.2 PROPOSED SYSTEM

The proposed method is to provide a fast and safe environment for toll collection and to automatically

control the vehicle movements at the toll stations. IR sensor is used to detect the vehicle and the Gate models are used here to open and close while the vehicle is entering or exit in the Toll Tax unit. The RFID reader is used to read the tag of the vehicles. The Vehicle information is stored in the microcontroller based on the TAG number. Based on that number the Tax amount for that vehicle will automatically transfer to the toll gate system. And that cost information will be sent through GSM modem to a mobile phone of the owner. The main objective behind this proposal is to create a suitable Automatic Toll Gate System to be implemented. However, this proposed system requires major changes in the infrastructure of the existing toll roads. In this project, we propose, analyze, and experimentally demonstrate a new localization problem found in many large scale WSN deployments: *the Wireless Localization Matching Problem* (WLMP). Here the locations of the sensor nodes are known *a priori*. However is the unique ID of the wireless sensor node which is located at each position. Essentially, the WLMP is a spatially embedded version of the celebrated *matching problem* of probability theory, A deck of *m* cards labeled 1 through *m* is shuffled randomly. A match occurs when the number on the card matches the card's position in the deck.

2.ARCHITECTURAL DESIGN

2.1 SYSTEM ARCHITECTURE

We propose a model, design and implementation of vehicle toll payment based on loT device. Such loT based payment system is based on source and destination point selection as well as calling a web service on a centralized web application. The web service call implies transmitting authorization data such as (hashed) user ID, vehicle category and license plate, as well as all desired toll payment information as JSON data. Afterwards, the web application processes the received data and realizes the payment electronically over an electronically (online) payment service. Such online payment service can represent the well-known and popular PayPal. In case of successful payment realization and on query request from IoT device, the web application responds to the request and transmits back the payment realization details for the specific vehicle (based license plate, vehicle category and user lD). After the payment confirmation and successful response, a possibility to drive through the toll stations or through the country (in case of vignette) without retention is considered and condition.

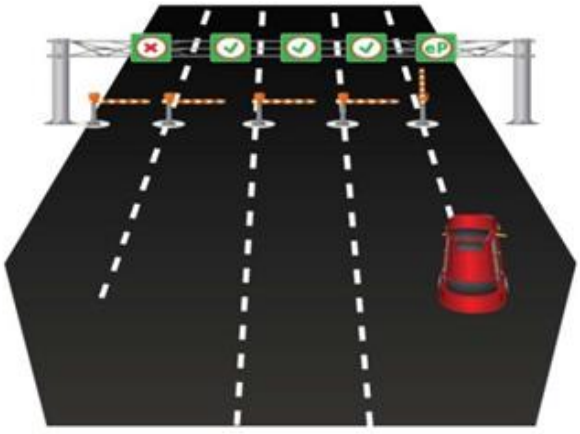

Fig 1: vehicle toll payment using IoT device

When a vehicle reaches the toll station at a specific distance, camera (on toll stations) scans the license plate and transmits the information to the local system which analyzes the payment detail for that vehicle based on license plate information. After successful payment approval, the toll ramp opens, which enables the vehicle driving through the toll station without retention. Analog approach for vignette payment, camera on or near the country border scans and sends the vehicle license plate to local system which examines the vignette payment.

2.2 HARDWARE ARCHITECTURE

2.2.1 Power Supply:

If you are considering making your own power supply then three components are needed: · Transformer · Bridge rectifier · Smoothing capacitor. The transformer's current rating a least 2/3rd 's of the stepper drive boards capability, so for example: The Rout Out CNC stepper drivers have a 2.5A limit therefore (2.5 / 3) X 2 = 1.66A If you had for example 3 boards (X,Y,Z) then this would be 1.66 X 3 = 4.98 A Total Current. The DC output voltage of the supply will be 1.4 times the transformer's ac voltage when rectified. For example: An 18 VAC secondary will provide about 25 VDC at the output of the smoothed supply. The bridge rectifier's voltage and current ratings must exceed what the supply will deliver. Finally the minimum filter capacitor size must be calculated.

2.2.2 GSM:

GSM modem allows the computer to communicate over the mobile network through calls, SMS and MMS messages. It consists of a SIM card and operates over a subscription through a mobile network. It is a highly flexible plug-and-play device capable of connecting to a PC or any microcontroller's serial port through MAX232IC. This IC is used to convert the TTL logic levels of the microcontroller to a RS232 logic level for enabling serial communication. GSM is a TDMA based wireless network technology developed in Europe that is used throughout most of the

world. GSM phones make use of a SIM card to identify the user's account. The use of the SIM card allows GSM network users to quickly move their phone number from one GSM phone to another by simply moving the SIM card.

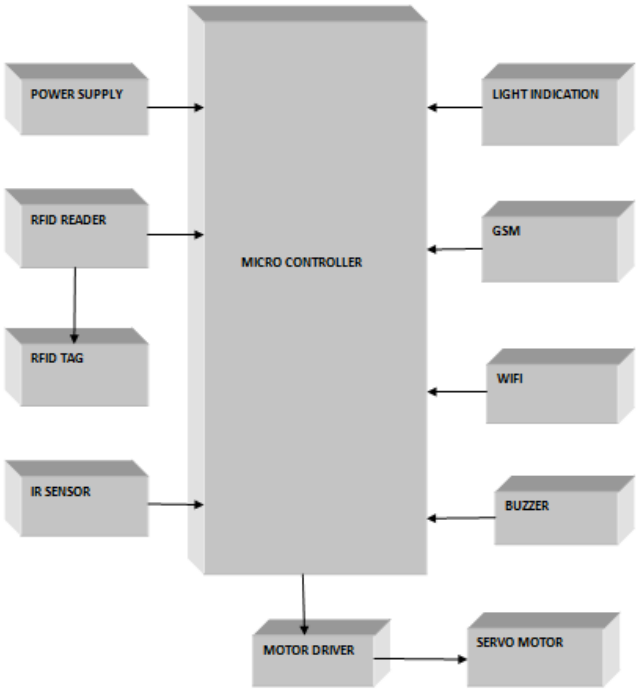

Fig 2: Basic block diagram of toll collection

2.2.3 MEMS Sensor:

Polysilicon springs suspend the MEMS structure above the substrate such that the body of the sensor can move in the X and Y axes. Acceleration causes deflection of the proof mass from its centre position. Around the four sides of the square proof mass are 32 sets of rad. These fingers are positioned between plates that are fixed to the substrate. Each finger and pair of fixed plates make up a differential capacitor, and the deflection of the proof mass is determined by measuring the differential capacitance. This sensing method has the ability of sensing both dynamic acceleration and static acceleration.

2.3 SOFTWARE ARCHITECTURE

While RF localization has come a long way, there are many unconventional localization problems which remain unexplored. In this project we have proposed a new type of localization problem for use in WSNs: the wireless localization matching problem (WLMP), which is a matching problem between perfectly known sensor node positions and their unknown IDs via wireless RF positioning methods. Examples of such scenarios are commonly found in real life, for instance during mass equipments installations in the commercial or Industrial buildings which are currently time and cost inefficient. Cloud becomes an ideal storage location for storing and processing IoT data but there are some problems to use the cloud for IoT data Storage. The main and major issue is security of cloud storage3. In many situation data collected from IoT devices is more sensitive or very important for the organization. When cloud storage is used, then organizations worried about the cloud security issues. This paper describes the some of the security issues which hampers the cloud and their resolutions which make sure to the organization that the data stored on cloud is secured. A first, sharing the computing resource with cloud providers, physical security is lost. Data is stored with the third party cloud provider therefore the user does not have knowledge where the data is stored and not have control over it. This issue can be solved by insuring secure Data Transfer. The second issue is preserving the integrity and truthfulness of the data. This issue can be handled by providing Secure User Interfaces. The third issue is, there may be the possibility that the privacy rights will not be followed by cloud service providers. This issue can be solved by applying cryptography techniques to data. We provide good software which insures about security of the cloud storage system, and then there is a no problem to accept cloud storage to store IoT data.

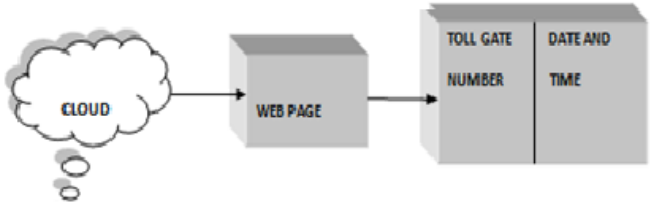

Fig 3: retrieval of information from cloud

3. SYSTEM WORKING

Internet of Things (IoT) aims to connect different physical environments, implementing different services such as measurement, control, analytics, reporting, etc. Such connectivity based on lightweight Internet protocols is not only constrained to a centralized system, it has the ability to interface other IoT devices together forming big and dynamic network.

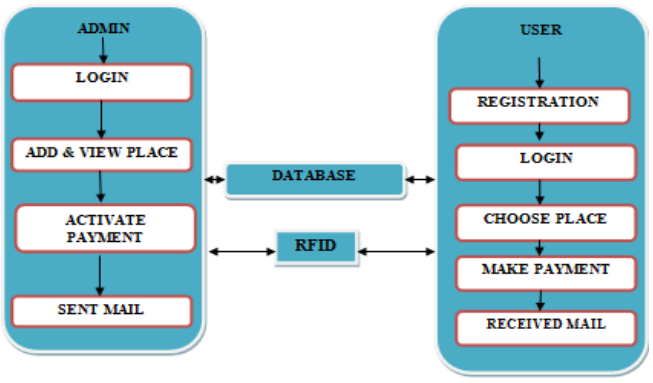

Fig 4: basic flowchart

In the proposed Architecture, IoT devices are placed to collect the data, if devices are not able to connect to the

internet and cannot transfer the data, and then gateways are used as intermediate between things and cloud to provide the needed connectivity. In the designed secure system, the administrator will define the roles according to the job functionalities played in the organization, then he/she adds the user in the system who wants to access the stored data from the cloud storage according to their needs. Administrator also creates one role manager and gives access rights to manage the roles of the user. The Role Manager allocates the specific roles to the user and has authority to remove the role assigned to the user. After that, the collected data from devices are encrypted by the administrator and stored it in to the cloud storage for the particular role so that only the users with appropriate roles can decrypt and view this data. The data collected from IoT devices is stored in encrypted format, therefore cloud provider is not able to see or read this data Besides the interface, a plain text file on local host device is used with inserted routes which represent the driving routes and correspondent information for only the purpose of toll payment When the driver in the embedded application specifies the required information, a search is started on this file which results in representing all possible routes with vehicle toll payment. Thereafter, the driver has the ability to select required driving routes for vehicle toll payment and confirm the request. The parameters license plate, vehicle category, user ID as well as toll payment details through all required driving routes are always sent (for ticket or vignette payment). Thereafter, the web application processes the request through an electronically payment service.

4. CONCLUSION

By practically implementing Smart card based Automatic Toll plaza System. We can provide a convenient transportation for the public i.e. we can avoid traffic congestion. It is the most efficient way of toll collection which can reduce the manual effort at toll plaza. We are avoiding the emergency vehicles such as ambulance, fire force etc. from the toll collection. In this busy world we give preference for time and efficiency, so for fulfilling this we can implement this kind of toll collection system. By doing automation of toll plaza we can have the best solution over money loss at toll plaza by reducing the man power required for collection of money and also can reduce the traffic indirectly resulting in reduction of time at toll plaza.

5. REFERENCES

[1] Daniel K. Fisher, Rapid Deployment of Internet-Connected Environmental Monitoring Devices, Advances in Internet of Things, vol. 4, pp. 46–54, (2014).

[2] Intel, Developing solutions for Internet of Things, White paper on Internet of Things, www.intel.com/iot. Macmillan, (1979).

[3] Amit Sangroya, Saurabh Kumar, Jaideep Dhok and Vasudeva Varma, Towards Analyzing Data Security Risks in Cloud Computing Environments, Springer-Verlag Berlin Heidelberg, pp. 255–265, (2010).

[4] O.Harfoushi, B. Alfawwaz, N.Ghatasheh, R.Obiedat, M.Abu-Faraj andH.Faris, Data Security Issuesand Challenges inCloud Computing: A Conceptual Analysis and Review, Communications and Network, vol. 6, no. 1, pp. 15–21, (2014).

[5] J. D. Bokefode, S. A. Ubale, S. Apte Sulabha and D. G. Modani, Analysis of DAC MAC RBAC Access Control based Models for Security, International Journal of Computer Applications, vol. 104, no. 5, October (2014).

[6] B. W. Lampson, Protection, ACM SIGOPS Operating System Review, vol. 8(1), pp. 18–24, January (1974), J. K. Wang, Xinpei Jia, Data Security and Authentication in Hybrid Cloud Computing Model, Global High Tech Congress on Electronics (GHTCE) on IEEEPublication, pp. 117–120, (2012).

[7] B. Katole, M. Sivapala, Suresh V. (2013, July). Principle Elements and Frameworks of Internet of Things. International Journal of Engineering and Science.

[8] Gubbi, R. Buyya, S. Marusic, M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements,and future directions", Future Generation Computer Systems.

[9] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)".

[10] R. Sandhu and Q. Munawer, The ARBAC99 Model for Administration of Roles, In Proc. of the 15th Annual Computer Security Applications Conference, Phoenix, Arizona, December (1999).

[11] R. Sandhu, E. J. Coyne, H. L. Feinstein and C. E. Youman, The ARBAC97 Model for Role-Based Administration of Roles, In Proc. of 2nd ACM Work-shop on Role Based Access Control, (1997).

[12] R. Sandhu and Q. Munawer, The RRA97 Model for Role Based Administration of Role Hierarchies, In Proc. of 3rd ACM Workshop on Role Based Access Control, (1998).
[13] Bhagyashri Katole, Manikanta Sivapala and V. Suresh, Principle Elements and Framework of Internet of Things, Research Inventy: International Journal of Engineering and Science, vol. 3, issue 5, pp. 24–29, July (2013).

[14] W. Stallings, Cryptography and Network Security Principles and Practices Fourth Edition, Pearson Education, Prentice Hall, (2009).

[15] Tingyuan Nie and Teng Zhang, A Study of DES and Blowfish Encryption Algorithm, IEEE Publications, (2009).

[16] Singh, S. Preet and Maini, Raman, Comparison of Data Encryption Algorithms, International Journal of Computer science and Communication, vol. 2, no. 1, pp. 125–127, January–June (2011).