Electronic Toll Collection using Secure Cloud and CPDP

Ayyappan B[1] Gladwin A[2]
[1,2]Assistant Professor
[1,2]Department of Information Technology
[1,2]Jeppiaar Engineering College, Chennai, Tamil Nadu, India

Abstract— *This paper shows how the radio-frequency identification (RFID) technology can be used to optimize the electronic toll collection in highways. RFID allows the automatic discovery of vehicle in the highway to collect toll for the vehicle and it is a cost effective technology. RFID technology along with cloud makes this cost effective. In cloud the computing resources that are delivered as services can be used by the end users over internet. Vehicles fitted with RFID tags are identified using RFID readers and the vehicles information present in the cloud will be used for deduction of amount. Security can be implemented using cooperative PDP (CPDP) scheme based on homomorphic encryption for credential details. Unregistered vehicles are scanned through the camera (using ALPR algorithm) and PT algorithm is used for matching it with the database.*
Keywords— RFID, cloud, CPDP, PT algorithm, ALPR etc

I. INTRODUCTION

The cloud computing is the next gen in the evolution of computing where it provide everything starts from application to infrastructure. The cloud can be referred as encompass everything and it can be characterised by three things scalable, on-demand and metered. i.e the computing power can be increased or decreased, it can be accessed on-demand and pay for the usage.

The Radio Frequency Identification (RFID) [5] is a technology that uses electromagnetic waves for transfer of data and identification of the tags. The RFID system comprises of RFID and RFID tags. The RFID reader is used for reading the content from the tags using radio frequencies. The tag is a small device comprises of an antenna, memory chip to store information and sometimes power supply. The tag consists of unique identification number and this number can be used for identifying the tag using the RFID reader.

Multi-cloud strategy uses more than one cloud services to minimize the risk of widespread data loss or downtime due to a localized component failure in a cloud computing environment. Such kind of failures can be occur in hardware, software, or infrastructure. A multi-cloud strategy also improves the overall performance by avoiding vendor independent and using different infrastructures to meet the needs of different partners and customers. The main goal of the system is to make use of multi cloud services instead of data center to store the credential information to make the transaction in electronic toll collection system.

To make this implementation successful the scheme called cooperative provable data possession [1] is used here. PDP [1] (provable data possession) is a technique for providing integrity for the clients online i.e. without download. CPDP [1] implemented here makes use of multi clouds services to provide scalable data access. RFID [5] tag is installed in every vehicle and the RFID reader will be s installed in toll gates. When the vehicle enters the Toll collection center the RFID reader recognize the RFID tag and the unique identification number will be used for the deduction of the amount for the vehicle. Security for the user's credentials in the multi-cloud environment can be implemented using CPDP. Implementation on multi clouds provides easy, efficiency and fast retrieval of data. Usage of clouds reduces the chance of losing data by hardware failures. The cost related to the creation of centralized data center is ignored when using multi-cloud services.

II. MOTIVATION

To afford a easy, scalable, automatic recognition and transactional technique for electronic toll collection in highways using cloud services to minimize or to avoid the congestion in toll gates. Maintaining the data in a secured cloud helps the toll operator for a convenient operation in the toll collection centers. The security for the data in the cloud is provided by different techniques such as encryption, homomorphic technique and so on to overcome security issues in the toll collection system.

III. INTELLIGENT TOLL COLLECTION WITH CLOUD SYSTEM

In order to reduce the emerging traffic in the toll collection centers this system uses different techniques. Sometime the delay is due to payment delay, this system helps in overcoming such issues. In the existing system it consists of servers connected to data center which overloads the network traffic which in-turn cause delays. For each usage transaction will be carried out in data center and account will be debited accordingly.

During the usage the connection is established for each usage which will cause delay in data retrieval process. There is a possibility in the loss of connection to the server due to network traffic and difficulty in managing may lead to failure of concurrency of the data stored. Possibility of hacking/ crashing of server is high. To address this problem we consider the implementation of intelligent toll collection system.

The Proposed system removes the drawbacks such as lack of security for credential information and the delay in accessing the data. The data about the users are stored in a text file and the Cooperative PDP [1] scheme is used here. The data about the users will be encrypted by using homomorphic encryption to provide security.

After the encryption process the data will be fragmented into different blocks and stored in multi clouds for ease of access and prevention from destruction of information. Implementation on multi-clouds strategy provides easy access, efficiency, safe and fast retrieval of data. It reduces the chance of losing data by hardware failures. To achieve this goal, TPA is created as a core trust base on multi clouds for the purpose of security. TPA acts as an intermediate, so that clients communicate only with TPA to get access rights rather than communicating directly with

the CSP (cloud service provider). Hence access to the data stored in clouds is restricted to the trusted users.

Hence the attack which is involved in PDP, data leakage attack and tag forgery attack [1] is prevented. To make data security stronger Homomorphic encryption is used, in which tag value is provided by the user and the TPA performs the encryption. Whenever user wants to download the details it must provide the tag value.

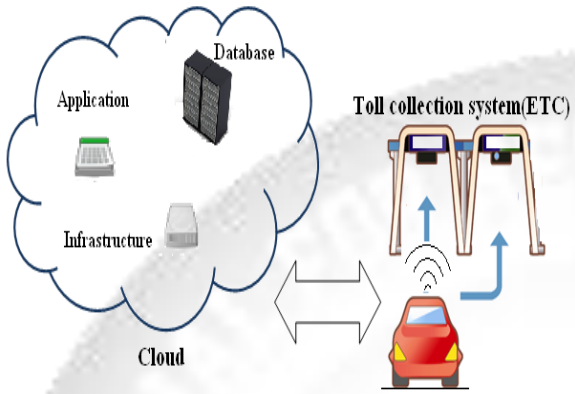

Fig. 1: Toll Collection system

IV. FUTURE ENHANCEMENT

As a future enhancement camera can also be used to capture the vehicle license plate. By using the information got from the registration or license plate of the vehicle, notification will be send to the owner of the vehicle in case of any violation. The character in the registration or license plate is recognized by algorithm called Automatic license plate recognition (ALPR) algorithm and Photograph to transaction matching (PT algorithm). In the ALPR algorithm the license plate of the vehicle is captured by using high resolution camera. The image is taken from different location and from different distance between camera and the vehicle.

The captured image is then converted into gray scale image and it is subjected to many processes to extract the license number of the vehicle. Along with the ALPR algorithm the PT algorithm [6] is also used for the recognition process. The RFID tag can also be used for the speed violation check. The speed of a vehicle can be tracked by deploying many RFID readers subsequently in the highway. The time taken by the vehicle to cross these RFID readers can be used to ascertain the speed of the vehicle and the penalty for speed violation will be deducted in case of registered user. If the vehicle is not having RFID tags, notification for speed violation and penalty will be send to the owner.

However the problem of Provable Data Possession (PDP) is also sometimes referred as Proof of Data Retrivability (POR) – has popped up in the research literature. The central goal in PDP is to allow a client to efficiently, frequently and securely verify a server – who purportedly stores client's potentially very large amount of data – is not cheating the client. In this context, cheating means that the server might delete some of the data or it might not store all data in fast storage, e.g., place it on CDs or other tertiary off-line media. It is important to note that a storage server might not be malicious; instead, it might be simply unreliable and lose or inadvertently corrupt hosted data.

An effective PDP technique must be equally applicable to malicious and unreliable servers. The problems further complicated by the fact that the client might be a small device (e.g., a PDA or a cell-phone) with limited CPU, battery power and communication facilities. Hence, the need to minimize bandwidth and local computation overhead for the client in performing each verification

V. CONCLUSION

In this article the implementation of intelligent toll collection system in the highways leads to a revolution in the traffic management. Implementing this system will minimize the average waiting time of a vehicle in a toll collection center in the highway. This system is a scalable one and it implemented by using multi-cloud technology will reduce the cost for installing and maintaining the Toll collection infrastructure.

REFERENCE

[1] DATA SECURITY THROUGH CPDP using homomorphic encryption.Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage Date of publication: Dec. 2012 Author(s): Yan Zhu
[2] Wu, N.C., et al., Challenges to global RFID adoption.Technovation, 2006. 26(12): p. 1317-1323.
[3] Asif, Z. and M. Mandviwalla, Integrating the supply chain with RFID: A technical and business analysis. Communications of the Association for Information Systems, 2005. 15(24): p. 393–426.
[4] Li, Zhekun, Application of RFID Technology and Smart Parts in Manufacturing, DETC2004, 2004; p. 2-7.
[5] TOLL COLLEACTION Using RFID RFID Technology Applied to Monitor Vehicle in Highway Date of Conference: July 31 2012-Aug. 2 2012
[6] PT and ALPR Algorithm A novel non-payment vehicle searching method for multilane-free-flow electronic-toll-collection systems, Date of Conference: 19-22 Feb. 2012 Author(s): Lin, L.R.