An Optimized Approach in Digital Gateway of Toll Tax Collection Using RFID Card

Abhishek Bajpai[1], Shivangi Nigam[2]
[1, 2] Dept. of Computer Application
[1, 2] SRMU, Barabanki, UP-225003

Abstract- *Emerging wireless technology can be effective for providing digital solutions to our day to day works and thus minimize the delay time. Wireless Digital solutions play a vital role in communication and security of our routine information. The digital innovations with the Internet-of-Things provide ease in various routines of our life. This ease can be improved by integrating cloud based application of these digital innovations. Cloud provides on-demand solutions and thus saving the time and money. This research presents a hypothetical model based on cloud to authenticate any human on toll plaza. The identification techniques can be implemented on various platforms. This study proposes LOCO-UID (LOCOMOTIVE USER IDENTIFIER) approach for authentication process. According to this model a user can be identified or registered only by AADHAR card.*

Keywords- Smartphone, Modules, Pocket Gadget.

I. INTRODUCTION

Smart Phones not only changed the way of communication but also modified the standard of living. Smartphone are part of our daily life now. According to recently made research there are 160 million smart phones users within the country which is likely to increase by 26% of CAGR by the end of 2017 [1]. This not only depicts a clear image of how much these small gadgets have influenced our life's rather it also shows how dramatically it is becoming important for the survival. Increasing demands are leading to introduction of more updates with these gadgets making them more efficient in performance in looks and performance. Smartness of these devices nowadays is just not limited inside the pocket rather they are also taking place of other gadget placed on the table (personal computers), carried as tracker or a camera showing a higher and better rate of peripheral support. These small gadgets run on operating system such as android, i-OS, windows, java, Linux, etc. enabling to run various programs and applications. The identification procedures of individuals at various places such as Tolls etc can be improved by introducing the idea of easing the process with the help of smartphones. In the current scenario maximum population is provided with unique identification numbers. The AADHAR can be considered as a global identity and can be linked for every individual. This research discovers various ways of identity creation. The main objective of this research is to generate an image of development of such software which uses Smartphone's for the generation of unique LOCO-UID of user which could be used at different level for the user identification and at same time reduces the problem of having multiple ID of a same user at different platforms for its verification process.

II. IDENTITY ESTABLISHMENT

It is mandatory for any utility providing department for subsidizing identity with the utility advantages enlistment. It is a tool for providing an exclusive batch to an individual which delineate his identity either in a computerized form or by any substantial means. Identity verification requires an individual to claims for his identity requiring a checkpoint for matching up with the exclusive batch provided to him. Thus, for every user should have a unique USER-ID where the connate could be established between the user and the utility provided to him which he demanded. For understanding this we can cast an example of a motor bike user, for riding a bike he has to carry a unique motor ID termed as driving license which incorporates his name, address, date of birth and his biometric used for his verification and type of vehicle he uses (geared or non-geared), with the time of validity is mentioned as utility advantage. The installation and authentication of such user ID's requires –

1. What is known to user

Such as user id, key, and any secret query. This can only be used as a part for computerized verification, as in case if done by any sensible mean it may lose its uniqueness.

2. What user is having

This is done by both computerized as well as physical means depending on batch provided. Here user carries some unique ID which is being provided to him by a substantial means such as- driving license, voter ID card, Aadhar-card, employee ID card or something like this which could be used for identification.

3. Who the user is

This can also be done by both computerized as well as physical means depending on batch provided. Such as- finger pattern, barcode, iris and facial recognition pattern, OMR and voice recognition. In case of physical verification, mostly photograph is being verified which is there on the batch provided to the user. For example- photograph on AADHAR card.

III. Current System Issues

1. Identity Generation Issues

- Numerous ID generated for particular user because of shortfall in the context of expertness in exclusive recognition.
- Reserved tags for different departments which can be operated only within that department and for a precise purpose.
- As number of identical and bogus identities are generated for a particular asset which conclude in leakage of utility advantages as it becomes inconvenient to identify the user.
- Raise number of forge activities as it is somewhat easy task for generating multiple Xerox copy of substantial ID proof.
- Declining rate in providing benefits to the users as there are cases of mismatching or irrelevant matching of utility provided to user from different programs.

2. Identity Verification Issues:

- Demand for costlier checkup installations with limited resources.
- Sometimes it is a tough job catching forged documents.
- In computerized verification it is a difficult job to recognize the user as there is no visual displayed except some cases where facial recognition pattern is being used.
- There is no machinery for the checkup to prevent identity misuse.

3. Identity holder Issues:

- Multiple steps involved in ID generation involving risk of carrying records for their verification.
- In case of computerized verification users have to remember different keys for different instances.

This paper introduces us with one more extraordinary feature of these Smartphone's by using it in user identification process. Different nation has their own way for identifying their citizens, some of them can be listed as: -INDIA – AADHAR/UID, PAN (Permanent Account Number), DRIVING LICENSE, PASSPORT, USA – SSN (Social Security number), CANADA - SIN (Social Insurance Number), UK-NINO (NI Number).

IV. PROBLEMS FACED IN DIFFERENT COUNTRIES

1. INDIA

- Multiple ID with time effective steps in generation of these ID.
- High renewal cost.
- Maximum cases of forgery registered because of ineffective management policies.

2. US

(Challenges Faced in SSN)

- Leaking of privacy related contents
- Chances of data being hacked

3. United Kingdom

- Difficulty in protecting privacy of citizens.

Increasing demand of a secure and unique identification technique not only creates a platform for the user to be protected instead it also gives opportunity to enjoy the different services which are being provided to him by the different utility providing agencies such as The Unique Identification Authority of India (UIDAI) [2] which introduced the Unique ID [3]. Use of smart phone technology and theories related to it in the field of user identification points out toward a new and more efficient emerging technology which would maximize in decreasing the rate of forgery as well as reduce the burden of multiple ID at multiple platforms.

V. PROPOSED MODEL

User's identity is basically categorized on the basis of its name, gender, age and addresses these ID as brought into the category of Uniquely Identified by combining these aspects with biometric aspects such as thumb expression and facial impression of the user. Now, it is possible to generate a digital ID of a user using these aspects.

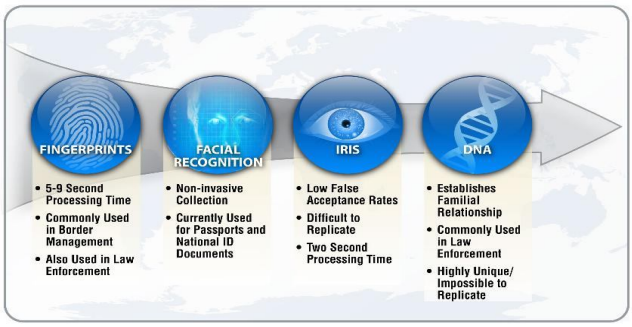

Figure 1. Various Authentication Methods

Various batches can be assigned to a single user such as-PIN, mobile/OTP, fingerprint, iris that can be used in verification process as per the service required. LOCO-UID is software for Smartphone that operates uniquely for identification of a user. As per the existing technique users are identified by different-different physical means which are to be carried at different instances at the time of verification increasing load to carry and risk of their security management. Sometimes it happens that there are cases of mismatching of data due to some default leading to trouble in verification process. LOCO-UID (LOCOMOTIVE UNIQUE IDENTIFIER) is a pre-programmed application for identification in Smartphone putting control regarding the information related to the user with cryptographic features.

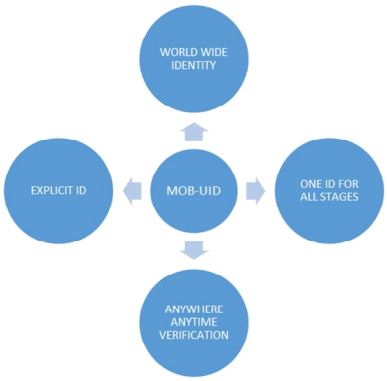

Figure 2. Diagram to Depict Various Benefit of LOCO-UID

Amit Krishnan, et all [4] proposed a centralized model for the Indian Public Distribution System (PDS) and states its benefits over the current system. The proposed system has its Point of Sale (POS) outlets centered on an E-Box 3310 MSJK device which runs an OS customized in Windows CE. The processor communicates with three different centralized databases to access different data associated with the customer. This communication is triggered by a UID (Unique Identification) smart card. Sherman Chow, et all [6] proposed A novel technique for protecting Identification Documents (ID) against forgery and tampering which virtually eliminates the possibility of card forgery or misuse. In study from [7] presented an approach to authenticating photo-ID documents that relies on pattern recognition and public-key cryptography and has security advantages over physical mechanisms that currently safeguard cards, such as optical laminates and holograms. Smartphone technology evolves fast, and its popularity increased grasping more attention among scholars. Fahad [5] discussed adoption and evolution of Smartphone technology. He discussed Smartphone technology, adoption of new technology and Information technology adoption theories and technology. From the previously mentioned system a need for a new and better system arrives which enable the efficient process of identification and reduce the possibility of identity theft and forgery with maximizing the use of unique identity for various areas of identification.

VI. SYSTEM DESIGN AND MODULES

The system design and modules of MOB-UID includes two different modules as discussed earlier in this report. One module for the registration process in which data is taken as input and a unique ID is being generated after this process and is being stored in the memory of the Smartphone which act as an identity for the user. Second module is a verification module used for identification process of user through locomotive unique identification. The user provides ID allotted by the Smartphone for verification. Thus, necessary checks will be made in central database after which the result will be displayed accordingly. Below are the details of modules including sum modules involved.

1. Enrollment Process

a) Enrollment Unit

The enrollment module registers individuals into system database. During this phase, a biometric reader scans the individual's biometric characteristic to produce its digital representation. This Biometric information and personal information about individual is stored in the system database.

b) Extraction Unit

This module processes the input sample to generate a compact representation called the template.

c) Encryption Unit

This module performs necessary encryption or data security measures on the template, which is then stored in a central database.

d) Smart Unit

This unit issues the MOB-UID to individual on their Smartphone.

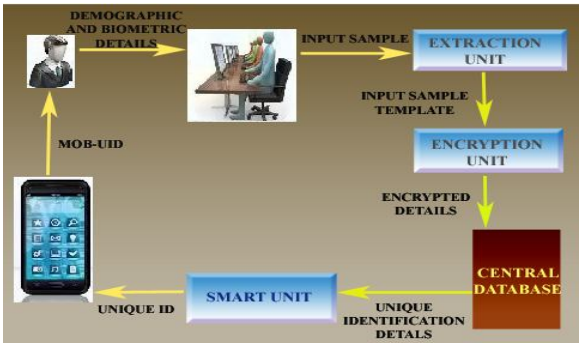

Figure 3. LOCOMOTIVE Unique Identification – Enrollment Process

2. Verification Process

a) Verification Unit

This unit receives the input from Smartphone.

b) Decryption Unit

Perform necessary decryption or reversible crypto operation on the input accepted from the Smartphone.

c) Matching Unit

This module compares the current input with the template. System performs identity verification, it compares the new characteristics to the user's master template and produces a score or match value.

d) Decision Unit

This module accepts or rejects the user based on matching score

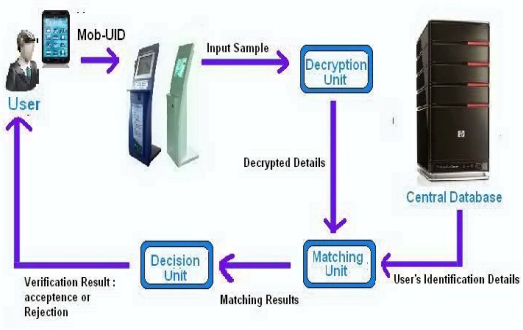

Figure 4. Verification Process

3. LOCO-UID Architecture

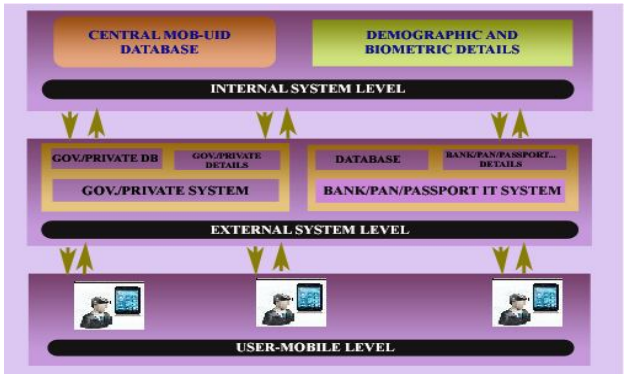

Figure 5. Different levels of abstraction in LOCO-UID ARCHITECTURE

This is a tree type architecture where we have different levels of abstraction which are internal system level, external system level and user-mobile level.

Here, internal level acts as a medium to interact between database of system and external interface hiding internal storage and functional complexity introducing channel between internal and external world. External level is a medium for internal and user-mobile level, here data is accepted and services are provided in user-mobile region. User-mobile level creates a bridge between the internal data storage and the external accessing environment. The external level uses the information stored in internal level to process and provide and interface to the user-mobile level. User-mobile act as medium for internal and external generating a view of system for the user helping him to communicate with the system.

VII. CONCLUSION AND FUTURE SCOPE

Today technology is taking its place in every sector of society; it is going under continuous process of updating where services can be made available to the majority considering the fact of presence of huge mass and its requirement for services. Mobile user identification is thus acting as a bridge in fulfilling gap generated between government, commodity and its need. It is digitized service providing scheme ensuring benefit for all and especially to those targeted section that really need these services. Thus, LOCO-UID builds up a stage where all the necessity regarding identification is in reach without much effort. But, for attaining such a big objective many changes are required with the installation of database and other infrastructure on which these are inclined. This could only come into action if and only if the commodity is provided with the latest gadget enabled with mobile verification application and once it is

introduced no one can stop the transformation phase of traditional world into digital world with more security and facilities. With fast growing mobile industry switching over maximum number of users from mobile phones to smart phone shows emergence of new era of technology with more powerful devices and application intended toward much more improvement and a better performance.

REFERENCES

[1] Last Access on : 27 August 2016,Latest mobile stats – Subscribers, [Online].Available, http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#subscribers

[2] Govt. of India, Unique Identification Authority of India Planning Commission, India. [Online]. Available: http://uidai.gov.in/, 2010

[3] Last Accessed on : 23 July 2015, The Unique Identification Authority of India website. [Online]. Available: http://uidai.gov.in/

[4] Krishnan, A., Raju, K. and Vedamoorthy, A., "Unique IDentification (UID) based model for the Indian Public Distribution System (PDS) implemented in Windows Embedded CE", 13th International Conference on Advanced Communication Technology (ICACT), pp 1441-445, 13-16 Feb. 2011

[5] Aldhaban, F. "Exploring the Adoption of Smartphone Technology: Literature Review", Technology Management for Emerging Technologies (PICMET), 2012 Proceedings of PICMET '12, pp 2758- 2770, July 29 2012-Aug. 2-2012

[6] Chow, S., Serinken, N. and Shlien, S.,"Forgery and Tamper-Proof Identification Document", nternational Carnahan Conference on Security Technology, Proceedings, pp 11-14, 13-15 Oct 1993

[7] Lawrence O'Gorman and Irina Rabinovich. 1998. Secure Identification Documents Via Pattern Recognition and Public-Key Cryptography. IEEE Trans. Pattern Anal. Mach. Intell. 20, 10 (October 1998), 1097-1102. DOI=10.1109/34.722623 http://dx.doi.org/10.1109/34.722623