# Two Factor Data Security Protection Mechanism for Cloud Storage System

**Prof.  P. P. Dandavate[1], Manas Pandit[2], Ashish Dalbhanjan[3], Vishal Dighe[4]**

*Department of Computer Engineering, TSSM's PVPIT, Pune University, India[1,2,3,4]*
*manaspandit555@gmail.com[1], ashish.dalbhanjan@gmail.com[2], vishaldighe209@gmail.com[3]*

*Abstract*— **Citizen Card system provides information about the citizen in any country. A citizen has unique id to identify to find out the personal information in each and every department or service whenever a citizen goes. If any citizen wants to utilize the service or utilities by government or private organizations, he has to go to each and every department with different id for the particular department. In citizen card system the citizen perform the all transactions based On Id. User performs like Banking, electricity, Banking Insurance , Tax, provident fund, Telephone, Gas, movies, Municipality, credit rating etc. Credit rating tells the behaviour of person whether citizen character is good or bad. This system not only helps us to know the information about the services or utilities but also it helps citizens save money and time**

*Keywords: Centralized networks, Distributed networks, Circuit-switching networks, Network communications, Store and forward networks*

## I INTRODUCTION

Citizen Card system provides information about the citizen in any country. A citizen has unique id to identify to find out the personal information in each and every department or service whenever a citizen goes. If any citizen wants to utilize the service or utilities by government or private organizations, he has to go to each and every department with different id for the Particular department. In citizen card system the citizen perform the all transactions basing on the id. He/she perform like Banking, electricity, Banking Insurance, Tax, provident fund, Tele-phone, Gas, movies, Municipality , credit rating etc. Credit rating tells the behavior of person whether citizen character is good or bad.

## II RELATED WORK

Citizen Card system, commonly based on SOA (Service-Oriented Architecture) has brought great comfort and convenience to the locals, drumming up the progress of Urban Information Construction. However, the application of citizen card system has not been popularized for some technical reason. This paper brief introduces its current situation, and illustrates the structure of the system according to the estimated effect and the adoption of SOA. On such analysis, the paper discusses the pros and cons of citizen card (system), pointing out the safety and management problems in details. In the end, the paper draws a future picture of citizen card (system), such as internet access and mobile-phone citizen card. In order to implement message processing edibility, easy scalability and fault tolerance, it created a general model that dynamically parsed the transaction message. Firstly, it offered a general definition for message processing and the relation between them secondly, it described the key objects of model and the relational model of them, furthermore, defined them with computer object-oriented technique, at last, the software realization given combining the key objects. The dynamic and flexible model services the transaction system which is mainly to process messages and already successfully applied to a citizen card system.

## III PROPOSED SYSTEM

In our system, we are going to enable the Administrator to perform operations basing on citizen id like gas agency, net banking, Personal Information, electricity bill, etc. thus providing flexibility and convenience to the final user.
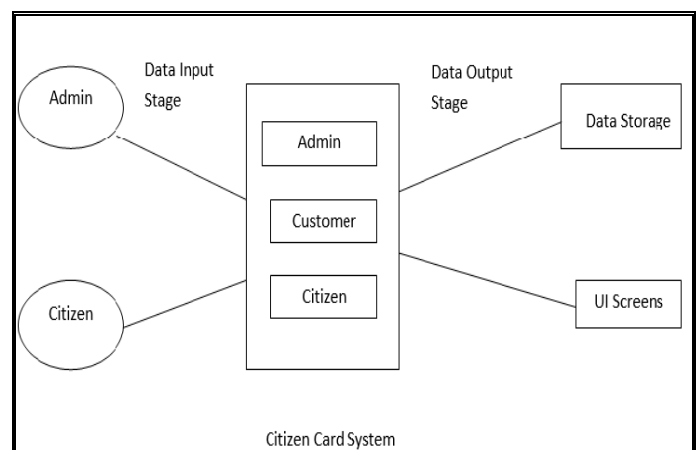
## IV SYSTEM ARCHTECTURE



*Figure 1:System Architecure*

1. **Guest:-**
- Should be able to search for Department details.
- Should be able to see the citizen status of request (Accepted/Rejected) for a Particular document.
- Should be able to see newly added departments in this site.

2. **Citizens (people):-**

- These citizens are authenticated to the website by providing the credentials which they got at the time of registration.
- Individual Profile Management for Each citizen is provided in this system by using that a citizen can update his details by using system interface and get approval.
- He can be able to secure login and give credentials.

3. **Administrator:-**

- He is treated as an owner of the web site.
- He should able to verify the information for a citizen to identify them.
- He should be able to edit, delete, and update Citizen Profiles.
- Should able to add/edit the Fields of particular Department like should able to add/edit the field along with Validation rules.
- He should also have rights to accept the registration of the Citizen based on their profile (unless the Citizen should not able to login to the site).

## V CONCLUSION

This project exhibits the design and usage of novel two-factor data security protection mechanism for cloud storage system, in which a data sender is allowed to encrypt the data with knowledge of the identity of a receiver only, while the receiver is required to use both his/her secret key and a security device to gain access to the data. Our solution not only enhances the confidentiality of the data, but also offers the revocability of the device so that once the device is revoked, the corresponding cipher text will be updated automatically by the cloud server without any notice of the data owner. Furthermore, we presented the security proof and efficiency analysis for our system.

## ACKNOWLEDGMENT

## REFERENCES

[1] A. Akavia, S. Goldwasser, and V. Vaikuntanathan, Simultaneous hard-core bits and cryptography against memory attacks, in Proc. 6th Theory Cryptography Conf., 2009, pp.474495.

[2] S. S. Al-Riyami and K. G. Paterson, Certi_cateless public key cryptography, in Proc. 9th Int. Conf. Theory Appl. Cryptol., 2003, pp. 452473.

[3] M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen, Certi_cate based (linkable) ring signature, in Proc. Inf. Security Practice Experience Conf., 2007, pp. 7992.

[4] A. Boldyreva, V. Goyal, and V. Kumar, Identity-based encryption with efficient revocation, in Proc. ACM Conf. Comput. Commun. Security, 2008, pp. 417426.

[5] H. C. H. Chen, Y. Hu, P. P. C. Lee, and Y. Tang, NCCloud: A network- coding-based storage system in a cloud-of-clouds, IEEE Trans. Comput., vol. 63, no. 1, pp. 3144, Jan. 2014.

[6] S. S. M. Chow, C. Boyd, and J. M. G. Nieto, Security-mediated certificate less cryptography, in Proc. 9th Int. Conf. Theory Practice Public-Key Cryptography, 2006, pp. 508524.

[7] Y. Dodis, J. Katz, S. Xu, and M. Yung, Key-insulated public key cryptosystems, in Proc. Int. Conf. Theory Appl. Cryptographic Techno., 2002, pp. 6582.

[8] L. Ferretti, M. Colajanni, and M. Marchetti, Distributed, concurrent, and independent access to encrypted cloud databases, IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 437446, Feb. 2014.