International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

E-Grievance: Centralized System for Municipal Corporation to Citizens by Hiding User Identity

Prof. Pandav R. M[1], Miss. Pansare Sonali D[2], Miss. Thakur Bhagyashri R[3], Miss. Kate Ashwini A[4]

[1,2,3,4]*SND College of Engineering & Research Centre, Yeola*

Abstract: *C*ity corporations in India are urban local government bodies that work towards the development of those cities which have a population of more than one million. Essential community services like public healthcare, sewage, electricity, road, etc. are the municipality's responsibility. The efficiency of municipal corporations in delivering their duties however, is abysmal Recently, Government is making the most of Information and Communications Technology to enhance the efficiencies and make possible new ways of delivering public services. For the government, the needs of people are to be identified and provide respective services. The proposed paper aims to overcome the problem faced by the citizen for the delayed response in resolving the several social issues that affects the rate of satisfaction of the complaints. This proposed work for the authentication purpose of the citizen to register their complaints a token is provided to keep user identity safe. A complaint form will be designed by keeping all the features of the Municipal Corporation. The user can register their complaint with their personal message in the complaint box. The municipal corporation can resolve their work based on the priorities. As the complaint status remains pending, it will be automatically forwarded to the higher official without the notice of the corresponding official. The result of this work is used to build a system to improve the complainant satisfaction.

Keywords: E-grievance Centralized System, Municipal Corporation, Departments, Citizens, Smart phone, Complaint Registration, Android API, Smart City.

1. INTRODUCTION

This project provides an online approach to local citizens of a particular city area to have better communication with the municipal authorities. This citizen can share their ideas, views, suggestions, rather complaints. Authorities can access all the complaint, suggestions from users and will give proper response. The system creates a user-friendly online interface for citizens to communicate with administrative body and reduce the distance and time barrier between citizens and administration. It consists of a web portal and an android app to register the complaints online from anywhere, at any time as well as money to go to an office for complaint registration .Three related concepts are encompassed by general scope of People's Corner. The first pertains to the replacement of personal visit to the office and registering complaint on paper, the second relate to complementary electronic strategy for the handling of a customer's complaint and third surrounds the process of taking actions by the government bodies against the complaints registered by the citizens. The user can click the picture of the venue of complaint and upload the same .Also the address of complaint location will be tracked automatically using GPS and Google maps, thus reducing user's overhead to typing the address.

Goals and Objective:

- To gain user anonymity.
- To increase the visibility to the intended client.
- To ensure that respective file is delivered to the authorities in any case.

2. LITERATURE SURVEY

1. "Using of an anonymous communication in e-government services: in the prevention of passive attacks on a network" Nowadays citizens live in a world where communication technologies offer opportunities for new interactions between people and society. Clearly, e-government is changing the way citizens relate to their government, moving the interaction of physical environment and management towards digital participation.

2. "Another Look at Anonymous Communication" Anonymous communication is desirable for personal, financial, and political reasons. Despite the abundance of frameworks and constructions, anonymity definitions are usually either not well defined or too complicated to use. In between are ad-hoc definitions for specific protocols which sometimes only provide weakened anonymity guarantees.

3. "A New Enhanced Secure Anonymous Communication with Authentication and Session Key Agreement in Global Mobility Network" Recently, several protocols have been

proposed to accomplish user authenticity with proper session key establishment in Global Mobility Network. Unfortunately, some them still suffer from various security threats and high computational complexity.

4. "Ant Colony Optimisation—A Solution to Efficient Anonymous Group Communication" Online Social Networks (OSNs) are the core of most communications nowadays, leading to possibly sensitive information exchange. Privacy is an important building block of free societies, and thus, for OSNs. OSNs function as group communication systems and can be build in centralized and distributed styles.

5. "STAC-Protocol: Secure and Trust Anonymous Communication Protocol for Internet of things" Security and privacy are prominent tasks in resource constrained devises in Internet of Things and Wireless Sensor Networks (WSN). Therefore, to ensure anonymity and trust, concealing nodes' real identity trust management are mandatory.

6. "PRACTICAL ANONYMOUS AUTHENTICATION Designing Anonymous Authentication for Everyday Use" We use authentication services many times a day. Without user authentication, it would be impossible to use email accounts, discussion boards, e-banking or even electronic communication. On the other hand, we release a lot of personal information during every authentication process. Our login can be linked to used services and assets by service providers.

3. EXISTING SYSTEM

To ensure anonymous user authentication ABSs this was also a centralized approach. A recent scheme decentralized approach and provides authentication without disclosing the identity of the users. In this system we are going to use KDC for generation of encrypted Tokens and encrypted keys. Key distribution is done in a decentralized way. There is KDC which generates encryption and decryption keys and keys for signing. Creator on presenting token to KDC it will provide secret keys and keys for signing. The cloud takes decentralized approach in distributing secret keys and attributes to user. System proposed a distributed access control mechanism in clouds. However, the scheme did not provide user authentication. The other drawback was that a user can create and store a file and other users can only read the file. Write access was permitted to users other than the creator. The cloud is also prone to data modification and server colluding attacks. Although Yang et al proposed a decentralized approach; their technique does not authenticate users, who want to remain anonymous while accessing the cloud. ABS (Attribute-based signature) is a protocol, In ABS, users have a claim predicate associated with a message. The claim predicate helps to identify the user as an authorized one, without revealing its identity.

4. PROPOSED SYSTEM

This proposed work is the extension purpose of the citizen to register their complaints a token is provided to keep user identity safe. A complaint form will be designed by keeping all the features of the Municipal Corporation. The user can register their complaint with their personal message in the complaint box.

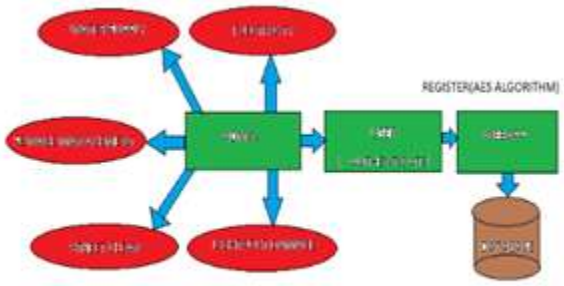


Fig. Proposed system architecture

The municipal corporation can resolve their work based on the priorities and the service for the complaint should be solved within the stipulated time. As the complaint status remains pending, it will be automatically forwarded to the higher official without the notice of the corresponding official. The result of this work is used to build a system to improve the complainant satisfaction.

- Token Generation: In this method, we will generate encrypted token by KDC. A security token may be a physical device that an authorized user of computer services is given to ease authentication. The term may also refer to software tokens. Security tokens are used to prove one's identity electronically. The token is used in addition to or in place of a password to prove that the customer is who they claim to be. The token acts like an electronic key to access something.

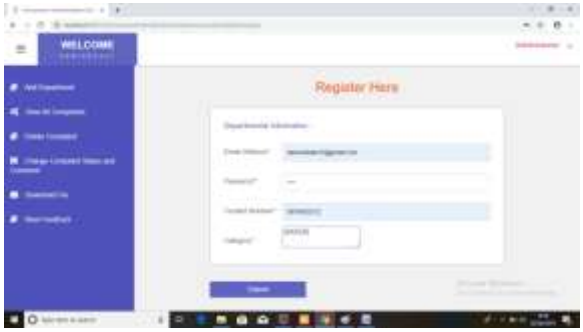
- Key Generation: After validating the tokens we will generate the encrypted key to the user. Key generation is the process of generating keys in cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted.

- Registration - Register user with name, email, Date of Birth and address. Token will be sent to specified email to authenticate user. If token is correct, then user will again get key on email, thereafter email and key will be the log-in credentials.
- After Logging In, user can upload files on Cloud and see list of uploaded files if uploaded before. Also user can share files from his uploaded file list through email.

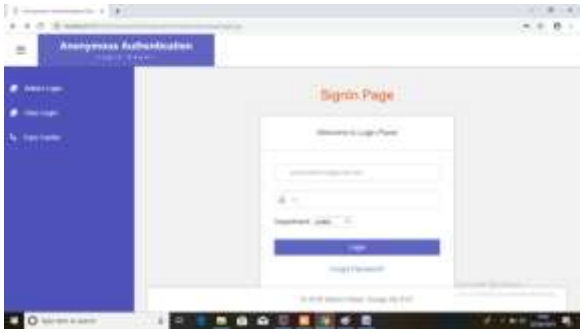
SCREENSHOTS:

1. ADMIN LOGIN:

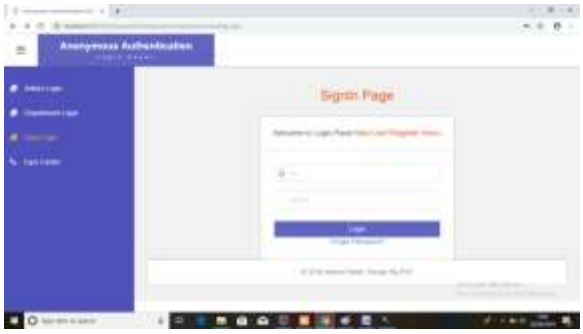
2. LOGIN PAGE:



3. DEPARTMENT LOGIN:



4.USER LOGIN:



5. MATHEMATICAL MODEL

Let S is the system for user to make complaint.

S = { I, O, F, DD, NDD, Success, Failure}

Where,

I = Input

I = {Register, Login, Complaint, Department }

O = Output

O = {Identity Encrypted, Complaint Solved }

F = { Register, Login, Complaint, Department, Identity Encrypted, Complaint Solved}

Success – All complaints solved successfully

Failure – problem in software

6. ADVANTAGES

- People get rid of traditional complaint system and can also keep track of their complaint.
- Irrelevant complaints can be blocked.
- User's identity kept safely.
- User can complaint without fear
- Complaint will get solve
- User can complaint department wise
- User can see others complaints
- User can comment to others complaint
- User can attach image, gif, video with the complaint

7. APPLICATIONS

- Medical Healthcare system
- Government security agencies

- Insurance Companies
- Mobile satellite communication systems
- Anti-ragging system
- Anticorruption system
- Education system.

8. CONCLUSION

This project provides a direct communication link between the citizen and the municipal corporation. This will help in registering the problems that one faces in a particular area. This also helps the municipal corporation to solve the grievance of the complainant based on priority and strengthens the reach and efficiency of the municipality. This system showcases the goal of a transparent government which works for the people rather than making them work.

REFERENCES

[1] Sushmita Ruj, Milos Stojmenovic, and Amiya Nayak, ˆa Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds, IEEE Trans. on Parallel and Distributed Systems, vol. 25, pp 1-11, 2014.

[2] H.K. Magi, M. Prabhakaran, and M. Rosulek, ˆaAttribute-Based Signatures,ˆa Topics in Cryptology CT-RSA, vol. 6558, pp 1-3, 2011.

[3] A. Beimel, ˆaSecure Schemes for Secret Sharing and Key Distribution,ˆa PhD thesis, Technion, Haifa, pp-1-115, 1996.

[4] S. Ruj, M. Stojmenovic, and A. Nayak, ˆaPrivacy Preserving Access Control with Authentication for Securing Data in Clouds,ˆa Proc.IEEE/ACM Intˆal Symp. Cluster, Cloud and Grid Computing, pp 1-8, 2012.

[5] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, ˆaToward Secure and Dependable Storage Services in Cloud Computing,ˆaIEEE Trans. Services Computing, vol. 5, no.2, pp 1-13, 2012.

[6] S.Seenu Iropia and R.Vijayalakshmi (2014), “Decentralized Access Control of Data Stored in Cloud using Key-Policy Attribute Based Encryption” in preceedings:International journal of Inventions in Computer Science and Engineering ISSN(print):2348-3431.

[7] M. Chase, “Multi-Authority Attribute Based Encryption,” Proc.Fourth Conf. Theory of Cryptography (TCC), pp. 515-534, 2007.

[8] Khan Safwan Mahmud and Kevin W. Hamlen, "AnonymousCloud: A Data Ownership Privacy Provider Framework in Cloud Computing, " Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 11th International Conference, pp. 170-176, 2012.

[9] A. Cecil Donald, A. Jenis and L. Arockiam, "An Authentication Mechanism to Enhance Security in the Cloud Environment," International Journal of Current Engineering and Technology, vol.4, no.5, 2014. Available at http://inpressco.com/category/ijcet

[10]] H. Ragib, "Security and Privacy in Cloud Computing," Johns Hopkins University en.600.412, 2010.