E-Governance: Centralized System of Municipal Corporation to Citizens

Ashwini Kate[1] Pansare Sonali[2] Bhagyashri Thakur[3] Prof. Pandav R. M.[4]
[1,2,3,4]SND College of Engineering & Research Centre, Yeola, India

Abstract— Municipal Corporations or city 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 (10 lakh). They are also called Mahanagar Palika or Mahanagar Nigam. Population levels in these cities are so high, and always on the rise, that the local government is very important in managing and maintaining them. 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 (ICT) 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 is the extension of Unique Identification number of the aadhar card 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 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.

Key words: E-Governance, Centralized System, Municipal Corporation, Citizens

I. Introduction

Now-a-days, the communication network is widely developed. Text and files can be shared in many forms. The investigation in cloud computing has received a lot of interest from educational and business worlds. In cloud computing users can contract out their calculation and storage to clouds using Internet. This frees users from problem of maintaining resources on-site. The services like applications, infrastructure and platforms are provided by cloud and helps developers to write application. The data is encrypted for the sake of secure data storage. The data stored in cloud is frequently modified so this feature is to be considered while designing the proficient secure storage techniques. In Online social networking access control is very important and only valid user must be allowed to access and store personal information, images and videos and all this data is stored in cloud. The goal is not just store the data securely in cloud it is also important to make secure that anonymity of user is ensured. Also we can use the benefits of cloud in providing certain control over corruption. People step back to take any step against corrupt actions due to fear of revealing their identity. For this anonymous authenticity is provided by cloud. In this paper, distributed access control that is only approved users with valid attributes can have entry to data in cloud. Also the identity of the user is kept a secret. Now another problem that arises is that what if some evidence is uploaded and the authentic user is not able to post it to the public due to some reason, then the evidence becomes of no use. To overcome this, in this paper we have added a timer function which will automatically upload the file after a certain period of time. There are many KDCs for key management because of this the architecture is decentralized. There is no access of data for users who have been revoked. The system is flexible to replay attacks. There is support for multiple read and write operations on data in cloud. The costs are analogous to centralized approaches and cloud performs the costly operations.

A. Goals & 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.

II. Literature Survey

1) "A Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds"- We propose a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the series without knowing the user's identity before storing data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. We also address user revocation. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.
2) "A Attribute-Based Signatures, a Topics in Cryptology CT-RSA"- We introduce Attribute-Based Signatures (ABS), a versatile primitive that allows a party to sign a message with fine-grained control over identifying information. In ABS, a signer, who possesses a set of attributes from the authority, can sign a message with a predicate that is satisfied by his attributes. The signature reveals no more than the fact that a single user with some set of attributes satisfying the predicate has attested to the message. In particular, the signature hides the attributes used to satisfy the predicate and any identifying information about the signer (that could link multiple signatures as being from the same signer). Furthermore, users cannot collude to pool their attributes together. We give a general framework for constructing ABS schemes,

and then show several practical instantiations based on groups with bilinear pairing operations, under standard assumptions. Further, we give a construction which is secure even against a malicious attribute authority, but the security for this scheme is proven in the generic group model. We describe several practical problems that motivated this work, and how ABS can be used to solve them. Also, we show how our techniques allow us to extend Groth-Sahai NIZK proofs to be simulation-extractable and identity-based with low overhead.

3) ”A Secure Schemes for Secret Sharing and Key Distribution”- A key distribution scheme for dynamic conferences is a method by which initially an trusted server distributes private individual pieces of information to a set of users. Later each member of any group of users of given size can compute a common secure group key. In this setting any group of t users can compute a common key by each user computing using only his private initial piece of information and the identities of the other $t - 1$ users in the group. Keys are secure against coalition of two k users, that is, even if k users pool together their pieces they cannot compute anything about a key of any t-size conference comprised of other users. In this paper, we introduce an algorithm for such perfectly secure scheme by using Pell’s equation.
4) ”a Privacy Preserving Access Control with Authentication for Securing Data in Clouds”- In this paper, we propose a new privacy preserving authenticated access control scheme for securing data in clouds. In the proposed scheme, the cloud verifies the authenticity of the user without knowing the user's identity before storing information. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.
5) ”A toward Secure and Dependable Storage Services in Cloud Computing”- Cloud storage enables users to remotely store their data and relish the on-demand elevated quality cloud requests lacking the burden of innate hardware and multimedia management. Nevertheless the benefits are clear; such ability is additionally relinquishing user’s physical ownership of their outsourced data that inevitably poses new protection dangers towards the correctness of the data in cloud. In order to address this new setback and more accomplish a safeguard and dependable cloud storage ability, we counsel in this paper a flexible distributed storage integrity auditing mechanism, employing the homomorphism token and distributed erasure-coded data. The counseled design permits users to audit the cloud storage alongside very handy contact and computation cost. The auditing consequence not only ensures forceful cloud storage correctness promise, but additionally simultaneously achieves fast data error localization, i.e., the identification of misbehaving server. Considering the cloud data are vibrant in nature, the counseled design more supports safeguard and effectual vibrant procedures on outsourced data, encompassing block modification, deletion, and append. Scrutiny displays the counseled scheme is highly effectual and resilient opposing Byzantine wreck, malicious data modification attack, and even server colluding attacks.
6) “Multi-Authority Attribute Based Encryption”- In an identity based encryption scheme, each user is identified by a unique identity string. An attribute based encryption scheme (ABE), in contrast, is a scheme in which each user is identified by a set of attributes, and some function of those attributes is used to determine decryption ability for each ciphertext. Sahai and Waters introduced a single authority attribute encryption scheme and left open the question of whether a scheme could be constructed in which multiple authorities were allowed to distribute attributes [SW05]. We answer this question in the affirmative. Our scheme allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. An encrypt or can choose, for each authority, a number dk and a set of attributes; he can then encrypt a message such that a user can only decrypt if he has at least dk of the given attributes from each authority k. Our scheme can tolerate an arbitrary number of corrupt authorities. We also show how to apply our techniques to achieve a multiauthority version of the large universe fine grained access control ABE presented by Gopal et al.

III. 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.

IV. Propose System

This proposed work is the extension of Unique Identification number of the aadhar card 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.

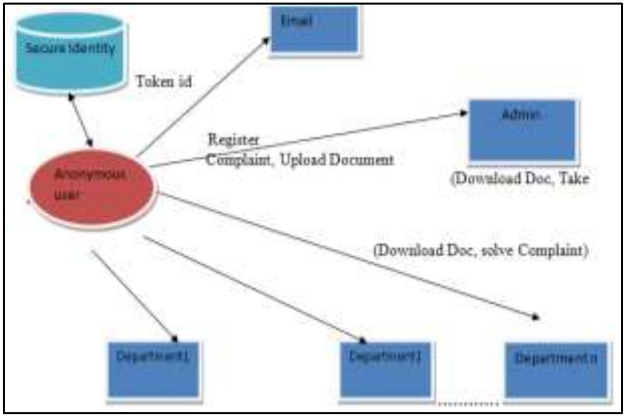

Fig. 1: Propose System Architecture

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.

A. *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.

B. *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.

C. *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.

V. 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

VI. 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.

VII. Applications

- Medical Healthcare system
- Government security agencies
- Insurance Companies
- Mobile satellite communication systems

VIII. 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] 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] 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] 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.