ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 7, July 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Smart City Framework Strategies for Citizen Centric Governance

Chilakalapudi Meher Babu[1]
Asst. Professor, Dept of CSE
Malineni Lakshmaiah Women's Engg. College
Guntur, India

Dr. Ashish B. Sasankar[2]
Professor, Head Dept of MCA,
G. H. Raisoni Institute of I.T, Hariganga Campus, MIDC
Nagpur, India

K. Prasuna[3]
Asst. Professor, Dept of ECE,
Vijaya Institute of Technology for Women,
Enikepadu, Vijayawada, India

Abstract: This framework design categories into various stages of the inner official management views associated with the information of the Government Services and user applications with different levels of abstraction. This Smart cities Framework mainly concentrated in various reports requested by the exploiter as well as higher authorities such as proposal wise details report, Government Services or Scheme wise details report, exploiter wise report etc. When the people apply for a scheme, his/her details will be stored in the database and sent to the Government Services or Government Scheme for verification. Government Services or Scheme people conduct a physical verification and get final approving authority and help him/her to approve or disapprove the person for the scheme. The same facts can be viewed by the people so that the people would get a clear picture of what is the phenomenon from time to time. So a secured and crystal clear system needed which enable an ordinary person to directly apply for a scheme and track the status from time to time and know whether he is entitled to receive the fruit or his application is rejected by the officials.

Keywords: smart cities, open data, citizen-centric challenges, citizen participation.

I. INTRODUCTION

An essential aspect of demonstration in massive stage of decentralized systems is the network infrastructure. Such as: several unrestricted services are being provided to the users through electronic means. To ensure easier and quicker access to unrestricted services in rural areas of the people, the government has established All Services Centers as universal service delivery route where the users can access all unrestricted services over the internet. The government has also launched a new proposal on mobile governance to provide all these services through mobile devices as well. The online and mobile based service deliverance mechanisms have generated the need for email authenticating the identity of the users so that each service or advantage reaches its proposed recipient in a protected manner. With efficiency, robustness, and less cost. In common, approaches towards addressing this problem in literature are of the following type:

1. Designing networks for specific domain dependent performance requirements,
2. Costing in search of specific optimal knowledge in network design,
3. Hardwork towards explaining the theoretical under pinnings or mechanisms that lead to Certain optimal behavior's in networks.

We move toward that is different from the above. While we consider recital requirements of specific domains as motivating examples, the intend process itself is domain independent and relies on optimization parameters abstracted in terms of optimal topologies through a process of evolutionary optimization.

II. Background

Due to isolated project implementations of the individual governance initiatives of various ministries/departments, the present authentication mechanisms are inadequate and disparate across various applications. As a result, there is not only a lack of uniformity in the authentication methods of various departments, but citizens also have to provide different kinds of identity proofs for accessing public services which are fairly similar in many cases in terms of their sensitivity. This scenario has led to sub-optimal end user experiences.

Government of India has conceptualized the Framework for e-Authentication that is intended to serve as the guiding document for all central and state ministries, departments and government agencies for implementing an appropriate authentication model for online and mobile based delivery of their services while maintaining uniformity and consistency across various authentication mechanisms.

III. Objectives

The framework enables a range of government departments and agencies to address the access management and authorization requirements associated with the deployment of e-authority applications and services. The objectives of its creation are as follows:

1. To provide a guiding framework to all government ministries, departments and agencies at both central and state stages for implementation of appropriate authentication processes and mechanisms as part of their service delivery strategy;
2. To define various types of authentication mechanisms and their usability in different scenarios that can be utilized by all government ministries, departments and agencies for electronically authenticating the users of government services;
3. To enable government ministries, departments and agencies to incorporate Aadhaar based authentication in their e-authentication mechanisms;

4. To enable consistency in the processes and procedures towards e-authentication of user identity;
5. To enable government ministries, departments and agencies to incorporate appropriate mechanisms for authentication of their websites to generate trust among the users;
6. To avoid duplication of authentication infrastructure and reduce the cost and efforts of the government ministries, departments and agencies in this regard;
7. To increase efficiency and maximize the ease of use in the e-authentication processes and mechanisms for all the stakeholders involved; and
8. To provide an implementation approach to assist the government ministries, departments and agencies in implementing e-authentication in the most appropriate manner.

IV. Policy Statement

Government of India shall adopt and deploy uniform electronic authentication mechanisms in a time-bound manner to ensure delivery of public services to the intended recipients. The Framework for e-Authentication lays down the following main policy measures:

Uniform electronic authentication mechanisms and processes shall be established to ensure electronic authentication of online and mobile users to facilitate access to and delivery of public services. The electronic authentication mechanisms shall incorporate Aadhaar based authentication.

ii. All government departments and agencies shall deploy e-Authentication processes as part of their service delivery strategy.

iii. All government Web sites shall be electronically authenticated in order to build trust among the users.

1. Identity Management

Identity management is a significant component of Framework to ensure trusted and reliable online delivery of government services to the authenticated users. Authentication and authorization should be considered within the context of identity management. Identity management can be described as "…the management of individual identifiers, their authentication, authorization, and privileges/permissions within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime, and repetitive tasks. ….Identity management (IdM) is a term related to how users are authenticated (identified) and their actions authorized across computer networks. It covers issues such as how users are given an identity, the protection of that identity, and the technologies supporting that protection (e.g., network protocols, digital certificates, passwords, etc.).”1 This includes single sign-on and password management functionality and a single point of administration for accounts hosted over one or multiple user stores.

2. Authorisation

Authorization is the process of verifying that a known person has the permissions and rights to perform a certain operation in an application. Authentication, therefore, must precede authorization. An effective access management system incorporates one or more methods of authentication to verify the identity of the user, including passwords, digital certificates, hardware or software tokens, and biometrics. Authorization governs what a user can access or do within an application. It lets the right users manage the content they have access to and the actions they can perform.

3. Credential Registration

Credential registration is the process which results in issuance of an e-authentication credential, using which an identity can be electronically verified. The credential can be of different strengths, e.g. a password, a token, a digital certificate, or a biometric parameter. The strength of the credential required will be determined by the sensitivity stage requirements of the application or transaction. Credential registration process may consist of a combination of the following elements:

1. Online/Offline process to allow users to register with the required identity and associated information

2. Creating user entries in an identity directory

The database includes users’ identities and associated information.

3. Issuing a credential to a user

This credential will be used in the e-authentication process. The directory keeps the details regarding the credentials.

4. Permission Assignment

In order to provide the user access to online services, appropriate permissions need to be assigned to the user as part of the permission assignment process after issuance of the credentials. Permission assignment may be implemented in one of the following ways –

- **As an extension of the credential registration process.**

Access permissions may be assigned to the user for services delivered by the government departments and agencies as part of the credential registration process.

- **As a separate activity performed at some time after registration.**

Access permissions may be assigned to the user based on a credential issued by some other agency at a later point of time.

5. Single Sign-On

Single sign-on is a specialized form of e-authentication that enables a user to authenticate once and gain access to the resources of multiple applications. With this property, a user logs in once and gains access to all systems without being prompted to log in again at each of them.

6. Implementation Approach

The implementation approach for the framework can be defined as a four-step process. It primarily addresses identity related solutions that include identity authentication, step-up authentication, and single sign-on across various government Web sites.

The steps of the implementation approach are as follows:

1) Determine the business requirements

a) Identify the services to be provided online

b) Assess the risk associated with each online service

c) Define the sensitivity stage for each online service

d) Identify the appropriate authentication mechanism

2) Select the registration approach

3) Incorporate at the application Stage

4) Review the e-Authentication solution

7. e-Authentication Assurance Stages

7.1 Internet Based Applications

There are five stages of application sensitivity for web based applications ranging from Stage 0 to Stage 4. The Stage 0 is the lowest stage whereas Stage 4 is the highest. Stage 0 will not require any form of authentication and will be used for providing public information over the web. All applications will therefore authenticate users using Stage 1 authentication by default. Sensitivity of the application, including URLs, should be defined during application development cycle. This would enable the application to call proper authentication mechanism at the right time. Application sensitivity stage will determine the calling of a suitable authentication mechanism from Stage 1 through Stage 4 at the appropriate stage.

A summary of the five stages is provided below:

7.1.1 Stage 0: This stage implies no authentication. The user can go to the government Web site and access all information that is made available for public use.

7.1.2 Stage 1: This is the basic authentication mechanism using username and password. The user could be provided the capability of self-registration by which she can generate a username/password. A self-service identity management mechanism will be used by the user if she forgets her password. It will avoid unnecessary calls to the helpdesk for resetting the user password. Aadhaar based verification involving matching of demographic information and Aadhaar numbers can also be used appropriately for verifying the identity of the users.

7.1.3 Stage 2: At Stage 2, a user will be able to prove her identity using OTP token along with her Stage 1 credentials (i.e., username and password or Aadhaar number and demographic information).

7.1.4 Stage 3: At Stage 3, the user would need to prove her identity through a hardware or software token (along with PIN) and username and password (i.e. through a two factor authentication process). For this purpose, token would be a digital certificate/digital signature or a smart card that would be required from the user end. Biometrics based verification using the Aadhaar authentication process may also be used at this stage.

7.1.5 Stage 4: At Stage 4, the user will prove her identity using two factor authentication which will necessarily include biometrics as one of the factors while the other factor could be either a token (hardware or software based) or a username/password. This is the highest stage of authentication security that would be available to a user. Biometrics based verification would be done in accordance with the Aadhaar authentication process.

7.1.6 Mobile Based Applications

For mobile based applications too, there are five stages of application sensitivity ranging from Stage 0 to Stage 4. The Stage 0 is the lowest stage of application sensitivity whereas Stage 4 is the highest. Stage 0 applications accessed through mobile will not require any form of authentication and will be used for providing public information over a mobile device. All applications will therefore authenticate users using Stage 1 authentication by default. Sensitivity of the application should be defined during application development cycle. This would enable the application to call proper authentication scheme at the right time. Application sensitivity stage will determine the calling of a suitable authentication mechanism from Stage 1 through Stage 4 at the appropriate stage. A summary of the five stages is provided below:

7.1.7 Stage 0: This stage implies no authentication. A user can avail the government service through various mechanisms such as Short Message Service (SMS), Unstructured Supplementary Service Data (USSD), Interactive Voice Response (IVR), etc. using her mobile phone and can access all information that is made available for public use.

7.1.8 Stage 1: This is the basic authentication mechanism using username and password. The user would receive the username & password after successful enrolment in e-Pramaan. The user will receive the password through SMS or print mailer. Aadhaar based authentication involving matching of Aadhaar number with demographics can also be used appropriately for verifying the identity of the users at this stage.

7.1.9 Stage 2: At this stage, a user will prove her identity using username, password and OTP. At the time of accessing a government service, the user will first provide her username and password or Aadhaar number with demographics and will then be prompted to enter the OTP.

Alternate option (only for smart phones): In this case, the user would need to prove her identity through username and password (or Aadhaar number with demographics) plus the random OTP generated through the OTP Generator (i.e., two factor authentication). The user will be required to download and install an "OTP Generator" from a trusted website (either provided by the government or by an authorised agency).

7.1.10 Stage 3: At Stage 3, the user would need to prove her identity through username and password plus a hard/soft token on a modified SIM or SD/microSD card/other medium containing the user's digital certificate along with PIN (i.e., through a two factor authentication). Biometrics based verification using the Aadhaar authentication process may also be used at this stage.

7.1.11 Stage 4 (for biometric enabled phones/devices): At Stage 4, the user will prove her identity using a two factor authentication which will necessarily include biometrics as one of the factors while the other factor could either be a hard/soft token (as mentioned in Stage 3 above) or a username/password. This is the highest stage of authentication security that would be available to a user. For this purpose, the user should have a biometric enabled phone/device. Biometrics based verification would be done in accordance with the Aadhaar authentication process.

7.1.12 "Fraud Management" Layer for Applications

Considering that the need for assurance of identity of users for applications falling under sensitivity stages 2 to 4 varies from moderate to very strong, there is a need for an additional layer of defence to prevent any kind of fraud. A "Fraud Management" layer will provide real-time protection against identity theft and online fraud. This layer will evaluate the fraud potential of online/mobile access attempts and assess the risk based on a broad set of variables. The "Fraud Management" layer will perform this task transparently without inconveniencing the legitimate users.

8. Privacy Implications

It will be the responsibility of the concerned government department or agency that aims to deploy online/mobile based applications to identify the privacy implications inherent in the proposed transactions and appropriately address the same.

9. Implementation Strategy

To ensure the implementation of the Framework in a time-bound manner, following actions will be taken.

1. Formulation of Guidelines:

Formulate detailed guidelines on the Framework to enable the government departments and agencies to select the right authentication mechanisms for e-authentication of users for delivery of their public services. It will also formulate detailed guidelines for authentication of government Web sites.

The guidelines shall help in ensuring security and confidentiality of data. The guidelines shall also help the government departments and agencies in applying a consistent approach in selecting the appropriate e-authentication mechanisms.

2. Creation of a Gateway:

The Gateway is the core infrastructure to enable electronic authentication of users for delivery of public services electronically to the intended recipients as well as to build trust of the users in the online and mobile environments. The Gateway will be used as a shared infrastructure by the central and state government departments and agencies. It shall incorporate the Aadhaar based authentication mechanisms provided by the UIDAI.

3. Creation of an Identity Directory:

The framework shall create identity directory(ies) to maintain the identity database. These identity directories (ies) may be built using the data collected, including the identity document numbers such as Ration Card Number, Voter Card Number, Driving License Number, etc., during the creation of the National Population Register (NPR) or by other government departments and agencies at central and state stages.

Gateway shall use the identity directory(ies), Aadhaar based authentication mechanisms and other suitable mechanisms such as those based on One Time Passwords (OTPs), digital certificates, etc. for authenticating users for delivering public services to the intended recipients through internet/mobile. Gateway may incorporate new technologies and processes for authentication in future.

4. Creation of a Facilitating Mechanism:

Establish and manage an appropriate facilitating mechanism to ensure implementation of the Framework by all government departments and agencies.

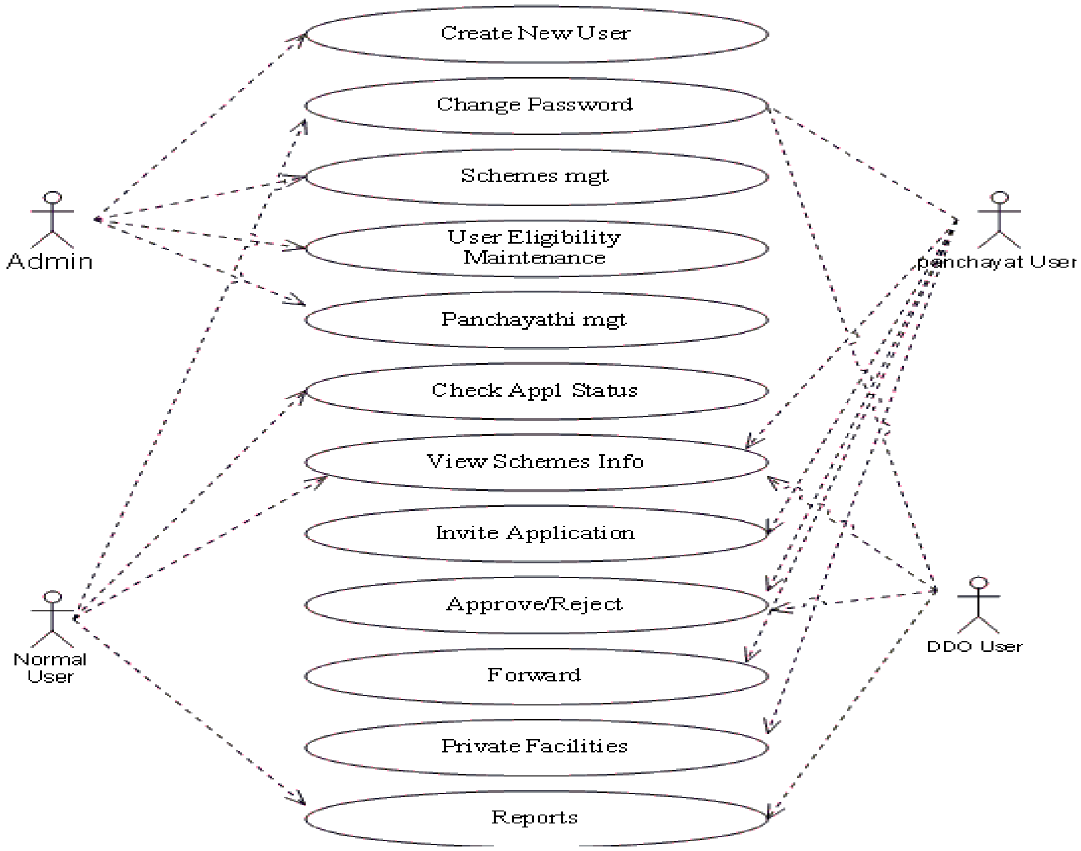
9.1 On-site command vehicle system:

The on-site command vehicle transmits important information and images collected at the site to the command center through communication satellites or wireless broadband networks. In the same way it also receives instructions and plans from the command management center, and issues instructions to personnel at the site. The on-site command vehicle system has capacity for communication activities as the communication base station and command center. Data required by on-site personnel can be accessed through the on-site command vehicle.

9.2 Comprehensive application of GIS:

Each department provides specialized images, which will be stored in the GIS data server through the GIS exchange system. For example, the specialized images supplied by the fire department contain information such as locations of fire hydrants and key firefighting authorities in the city; the specialized images from the health bureau contain information such as locations of hospitals and blood banks.

The system ultimately provides users with clarified information about different specialized images, as well as data signs on the map, for example, a sign or label indicating the location of a disaster site.



References

1. Denhardt, Robert B., and Janet VinzantDenhardt. "The new public service: Serving rather than steering." Public administration review 60, no. 6 (2000): 549-559.
2. Layne, Karen, and Jungwoo Lee. "Developing fully functional E-government: A four stage model." Government Information Quarterly 18, no. 2 (2001): 122-136.
3. Presthus, Robert V. "Weberian v. Welfare Bureaucracy in Traditional society." Administrative Science Quarterly (1961): 1-24.
4. Fang, Zhiyuan. "E-government in digital era: concept, practice, and development." International journal of the Computer, the Internet and management 10, no. 2 (2002): 1-22.
5. Bailey, Kenneth D. “Methods of Social Research”.4th edn. New York: The Free Press. 1994.
6. GoB (Government of Bangladesh) (GoB). “The Right to Information Act, 2009.” Dhaka: Government Publications
7. Bhuiyan, Shahjahan H. "Modernizing Bangladesh Public Administration through e-governance: Benefits and Challenges." Government Information Quarterly 28, no. 1 (2011): 54-65.
8. Rajon, SA Ahsan, and Sk Ali Zaman. "Implementation of e-governance: Only Way to Build a Corruption-free Bangladesh." In Computer and Information Technology, 2008.ICCIT 2008. 11th International Conference on, pp. 430-435. IEEE, 2008.
9. Ndou, Valentine. "E-government for Developing Countries: Opportunities and Challenges." The Electronic Journal of Information Systems in Develo ping Countries 18 (2004).
10. Islam, M. Sirajul, and ÅkeGrönlund. "Agriculture Market Information e-service in Bangladesh: A Stakeholder-oriented Case Analysis” Electronic GovernmentLecture Notes in Computer Science, Volume 4656, 2007, pp 167-178.
11. Ntaliani, Maria, ConstantinaCostopoulou, SotiriosKaretsos, EfthimiosTambouris, and KonstantinosTarabanis. "Agricultural e-government services: An implementation framework and case study." Computers and Electronics in Agriculture 70, no. 2 (2010): 337-347.3.
12. Ali, Shahed: “Success of Digital Bangladesh” (in Bangla). The Daily BhorerKagoj (Bangla Newspaper), 2010, January, 29.
13. Karim, Mohammad Rezaul. “Public Education Spending and Income Inequality in Bangladesh”.International Journal of Social Science and Humanity , Vol. 5, No. 1 (2015):75-79

AUTHOR(S) PROFILE

Chilakalapudi Meher Babu, did his M.Tech in Computer Science and Engineering from Jawaharlal Nehru Technological University, Kakinada, Andhra Pradesh (INDIA) and pursuing Ph.D in R.T.M. Nagpur University, Nagpur(India). He has 9 National and International Journal Publications to his credit. Currently he is working as Assistant Professor in the Department of CSE of Malineni Lakshmaiah Women’s Engineering College, Guntur, AP (India). His area of interst in research includes Network Intursion Detection System on Wireless Lan’s, IP Address, Routing Algorithms MANET’S and Database etc.,

Dr. Ashish B. Sasankar, did his MCA. M.tech (CSE), M.Phil. (Computer Science) & Ph.D. in Computer Science from R.T.M. Nagpur University (India). He has a rich experience of 16 years in the field of Education. Currently, he is the Head of the Department of MCA in the most prestigious G.H.Raisoni Institute of information Technology [GHRIIT], Nagpur [India]. He is a Ph.D Guide for Computer Science in the Faculty of Science in R.T.M. Nagpur University, Nagpur (India) and guiding many of his research scholars doing their Ph.Ds in Computer Science in R.T.M.Nagpur University, Nagpur. He has 40 National & International Journal Publications to his credit. He is a Member of the IEEE and CSI.

Ms K. Prasuna, working as Assistant Professor in ECE department in Vijaya Institute of Technology for Women, Vijayawada. She has more than 5 years of teaching experience. Her areas of interest are Digital Signal Processing, Wireless Communications, Image Processing and Wireless Networks.