Middle-East Journal of Scientific Research 24 (6): 1971-1976, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.24.06.23579

Offline Security Gate Operation In (ICMS) Identity Card Management System Using Aadhaar ID

[1]V.S. Raghunathan, [2]S. Kanaga Suba Raja and [3]S. Divya

[1]Research Scholar, Dr. MGR Educational and Research Institute,
Senior Technical Director, National Informatics Centre, Chennai, India
[2]Associate Professor, Information Technology, Easwari Engineering College, Chennai, India
[3]M.E. Software Engineering, Easwari Engineering College, Chennai, India

Abstract: e-Governance is achieved by applying information and technology by government to enhance the efficiency and effectiveness for providing services around G2G, G2C, G2E, G2B. The ultimate goal of e-Governance is to enable quick decision making, quick implementation and thereby achieves optimization of resources. Thus e-Governance demands a quality service hence the objective is to provide an optimized effective service delivery and reduce manpower. The paper proposes anOffline security gate operation in Identity Card Management System using Aadhaar integration aims at optimizing the verification process through online for entry/exit purpose. The integration of Aadhaar ID in visitor pass management portal to fix appointment through registration anytime/anywhere from India and also Offline security gate operation is going to be created to work independently in both offline/online for automatic updating of information about the individual consulting the Unique Identity Authority of India server for the first time through online and saves the information in the local database and offline accessing can be done when the person enter or exit at the security gate for the next time where connectivity is missing using single universal Aadhaar ID through Aadhaar scanning to reduce the manpower and high cost. The proposed system enables authentication to be registered with the Aadhaar id, validated and proper identification to be done in a secured way for entry/exit purpose.

Key words: e-Governance · Interoperability · Authentication · Offline agent · Aadhaar id

INTRODUCTION

The e-Governance platform delivers effective Government Services to the society. This e-governance platform creates independent services across many departments. The eSDP platform enables the service delivery life cycle to be optimized by re-using the common services and components [1]. Security gate operation in ICMS is provided by the Aadhaar integration with the help of an offline agent. Interoperability and Reusability between departments are enhanced by using the single unique identity as a proof across the departments and providing fastest verification mechanism by assigning Unique Id where it encrypts and encodes the same in light weight QR barcode [2]. Software agents are defined as being a software program that can perform specific tasks and it is designed, developed, deployed in a specific platform for a user and permits the task to be performed automatically [1]. Agent works in two ways, interactive agent and non-interactive agent. In every domain of operation it acts as a pivot element in optimizing the cost, time and resources. The participating domains include federated inter departments and other departments who shares the services in eSDP platform [1]. An agent Supports Parallel processing and autonomous task execution in a Distributed information retrieval and storage from the hosted repository. System requirements are configured by adapting specific part of the e-Governance Standards in order to provide commonly Shared resources, faster, improved and efficient services. The paper proposes the optimization of resources to be achieved with agents using identity card management system in e-Governance service delivery platform. The development and testing of agents are beyond the scope of this paper.

Drawbacks of the Existing Model of (ICMS) Identity Card Management System:

Corresponding Author: V.S. Raghunathan, Research Scholar, Dr. MGR Educational and Research Institute,
Senior Technical Director, National Informatics Centre, Chennai, India.

- Identity card management system (ICMS) in the security gate is only browser based connected frontend where it works only through online.

- In order to overcome online working in ICMS an agent is going to be created to work independently in both online/offline.
- The ID cards have two dimensional (2-D) QR BARCODE.
- The 2D QR barcode has an encrypted data, which is then converted into a decrypted data and sends to the server to get validated and issues detailed information about the individuals [3].

Benefit of Identity Card Management System: The following are the beneficial factors of ICMS

- Automatic updating of information about individual to the database.
- Anywhere and anytime authentication using Aadhaar card.
- Single unique ID therefore reduces in maintaining different ID proofs.
- One unique number to all citizens increases the security and verification process in a genuine manner [4].
- Aadhaar ID integration in the ICMS issues the detailed information about the individual for entry/ exit purpose through offline with the help of an offline agent.
- Aadhaar card for visitor's and instant booking to get entry pass reduces the cost and time.

System Architecture

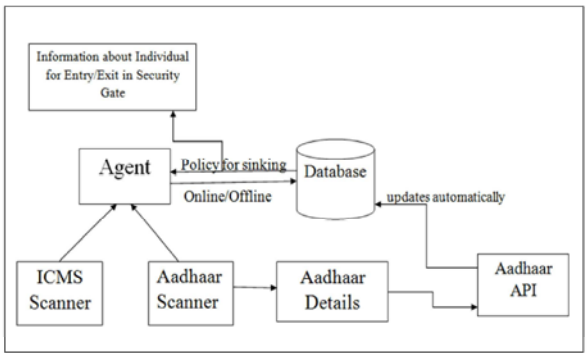

Fig. 1: Architecture Diagram

Agent for security gate operation in identity card management system using Aadhaar integration for online booking and instant booking of an appointment in ICMS visitor pass management portal, where we need to enter our Aadhaar number and mobile number to get the onetime password to retrieve the data's from the UIDAI server and automatically append on the corresponding values to get the instant visitor pass, where the agent will also work independently in both offline/online for automatic updating of information about the individual consulting the UIDAI server online for the first time and saves the information in the database and offline accessing can be done when the person enter or exit at the security gate for the next time where connectivity is missing. Therefore this measure effectively reduces the resources such as time and cost.

E-Governance Service Delivery using Aadhaar UID

Inter-Operable Identification: Interoperable service provide proper identification to the individual where UID is linked to passport, driving license, PAN card, voter ID for entry/exit purpose at the security gate in the absence of any identity proof. Interoperable identification has become a key imperative for efficient and timely delivery of services across various departments [5]. A unique framework allows secured exchange of information between various departments, while it also ensures genuineness of data.

ICMS as a Reusable Product: Single System for managing the entire organization operating from multiple locations. Admit Cards/Entry Pass can be issued to outsourced Agency employees, visitor's, maintenance people and other person's for entry and exit purpose.

ICMS as Software as a Service: In Software-as-a-Service (SaaS) model, the applications that are hosted online/offline enabling them to lower their costs, manpower and integrate easily with their existing data and systems. Identity Card Management System (ICMS) is offered as a SaaS service from Service Delivery Platform. As a SaaS Service, ICMS is instantly made available for a new organization or department with the resources required and the application can go online/offline. The integration of Aadhaar ID in visitor pass management portal to fix appointment through registration anytime/anywhere from India and also Offline security gate operation is going to be created to work independently in both offline/online for automatic updating of information about the individual consulting the Unique Identity Authority of India server for the first time through online and saves the information in the local database and offline accessing can be done when the person enter or exit at the security gate for the next time where connectivity is missing using single universal Aadhaar ID through Aadhaar scanning in order to reduce the cost and time.

Agent Lifecycle Model

Fig. 2: Agent Lifecycle Model

An agent is a computer system which is capable of performing actions in the environment automatically in order to meet its design objectives [6]. The architecture of agent manager provides a variety of processing like request form, visitor registration, review and approval, print visitor pass, offline scanning, validates and authorize, automatic updating where coining all together it becomes the execution cycle for creating the agent lifecycle [7].

Components of Agent Model: Request manager classifies the web services to define whether it is a push data or a pull data [8]. Web services is said to be a push data where insertion of data's are done in the databases [9]. Web services is said to be a pull data where selection of data's are done in the databases. Database manager provides basic database management functionalities including creation and maintenances of databases [6]. Database managers have several capabilities including the ability to backup and restore, attach and detach, create and delete the databases.

The Query Builder allows building complex SQL statements programmatically. It automatically fetches the SQL data's from the aadhaar database and helps to store in the local database of the ICMS. It offers automatic database abstraction, which integrates into multiple database platforms [10].

Test services in which it provides a quality assurance and conformity assessment services to create a quality web service.

eSDP is to deploy a service based platform to assess G2C,G2E and G2G with interoperable sharing of services between many departments. The eSDP is characterized by fully independent platforms that enable users to transfer between various departments. Thereby enabling the services for any time anywhere service delivery to the citizen, a common Esdp platform is being created [1]. Managing an agent provide an interface to perform various operation and it also manages the activities like enable the services, disable the services, start and stop of the services.

Verification Service in e-SDP: Verification services for each domain is added in the e-SDP platform and the identity verification is directed to the respective domain and the identity is assured of the Genuineness [11]. They can set rules and regulation about services registry then authorized used in the service registry. The delivery channels include Government Intuition, secretariats, Bhavans, educational institutions, hospitals etc.

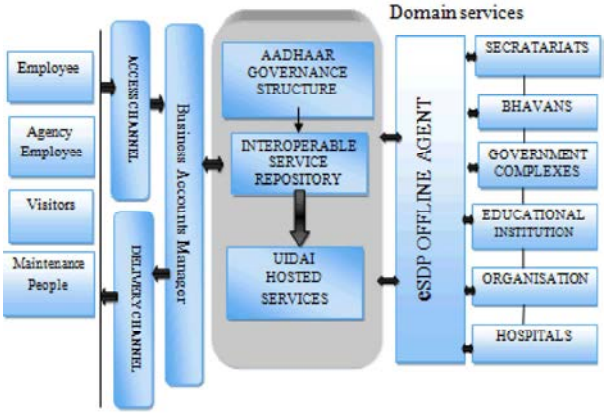

Fig. 3: eSDP Architecture

2-D Barcode Encrypted Data: 2-D Barcode Encrypted Data is the conversion of secured data into another form, called cipher text, which cannot be easily understood by anyone except authorized parties [2]. Encrypted data can be store in the Barcode and while scanning it connects to online/offline. In case of encrypted-ID, there will be a agent program to decode by sending to the server and fetches the validated information [12].

QR Barcode: QR barcode is type of matrix Barcode which is capable of handling a data such as numeric and alphabetic characters. Data can be restored even if the symbol is partially dirty or damaged [13]. QR Code is capable of 360 degree (Omni-directional), high speed reading.

Authentication: Authentication, where the credentials provided are matched to those on the aadhaar database of authorized users' or within an authentication server [11]. If the credentials match, the process is completed and the user is validated and verified with genuine information. for access in the security gate for entry/exit purpose.

Service design Achieved through CbC: NIC has developed many web application services [1] and it was noted that the requirement, design, development and the deployment phase are time consuming. The requirements of a new system is gathered and defined followed by the other phases and this procedure repeats for every new requirement.

- Online and Offline mode operations are supported.
- Authentication and authorization features like no authentication, simple authentication, multi-factor authentication.
- Photo capture, photo capture size is available.
- Geo-location based location services, range services features are supported.
- Allows customization for web applications.
- Selective master download and multiple master download features are provided.

Aadhaar ID: Unique Identification Number which was renamed as Aadhaar number provide to every indian resident for identification purpose to prove the genuineness of the person for entry/exit purpose. Authenticates against resident data in UIDAI'S server.

Agent Service Achieved Through cbc: An agent is a computer system that is situated in some environment which is capable of autonomous action in the environment in order to meet its design objectives [14]. The architecture of agent manager provides a variety of processing like request manager, database manager, query builder, test services, deploy, enable services and manage where coining all together it becomes the execution cycle for creating the web service [7].

Components of Agent Model: Request manager classifies the web services to define whether it is a push data or a pull data. Web services is said to be a push data where insertion of data's are done in the databases. Web services is said to be a pull data where selection of data's are done in the databases. Database manager provides basic database management functionalities including creation and maintenances of databases. Database managers have several capabilities including the ability to backup and restore, attach and detach, create and delete the databases.

Test services in which it provides a quality assurance and conformity assessment services to create a quality web service. e-governance service delivery platform is to deploy a service based platform to assess G2C,G2E and G2G with interoperable sharing of services between many departments. The eSDP is characterized by fully interoperable and integrated channels that enable service users to transfer between channels and experience seamless services [1]. Managing an agent provide an interface to perform various operation and it also manages the activities like enable the services, disable the services, start and stop of the services.

Web Service Functionality: The e-Governance services provide variety of application services to stakeholders. Multiple system components are integrated to deliver the application services. The major steps involved in the web service life cycle model are requirement specification, design, web service creation, web service integration, web service registration, web service testing and security audit.

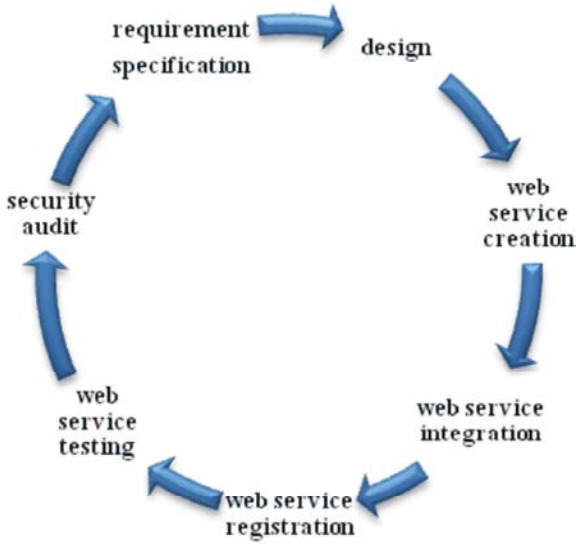

Fig. 4: Web Service Life Cycle Model

The Agents receive the requirements provided as input and processes these requirements as programmed to create a service ID [5]. The inputs are then passed as parameters to get the required information. The final output generated after the process completion are web services.

The agents have the capability to act as the query builder to fetch the information from the domain server and to execute these queries [11]. The output generated web service can be verified for the format and thereby allows the services to maintain the standardization. The agent should be programmed with the below requirements.

- Register ICMS Service ID, Service type(Master, Transmission, Multi-media, Dashboard etc.), DescriptCion, Authorization, Output format, filter conditions(if any), sort order(if any).
- Agent on multiple platforms (PHP).
- UI for Agent user client to configure, enable, test, deploy, buffering and monitor registered requests.
- Invoke APACHE2 Services.
- Configure APACHE2 Services.
- Security fixes for APACHE2 Services.
- Deploy registered requests & Service requests.
- Deploy the status of registered requests.

The agents are built from components that are customizable and reusable [8]. These agents constructed using the reusable components are hence more reliable. The approach allows configuration of Well-defined components and the relationship between them by reducing the construction of an agent.

Assuming that there are 'n' Processes (p1, p2, p3….pn), cost (c1, c2, c3…cn) and time (t1, t2, t3….tn) then the time taken for the existing application is

$$\sum_{i=1}^{m} p_i * t_i * c_i . \quad (1)$$

Re-engineering the application applying construction by configuration using the agent services reduce the number of process to produce the XML payloads.

If process is reduced from m to n and then time taken for the proposed application is

$$\sum_{j=1}^{n} p_j * t_j * c_j, n<m \quad (2)$$

Now the time saved in the proposed application using the Agents services is

$$\sum_{i=1}^{m} p_i * t_i * c_i - \sum_{i=1}^{m} p_j * t_j * c_j, n<m \quad (3)$$

CONCLUSION

This paper proposes the agent for security gate operation in identity card management system using Aadhaar integration for online booking and instant booking of an appointment in ICMS visitor pass management portal, where we need to enter our Aadhaar number and mobile number to get the onetime password to retrieve the data's from the UIDAI server and automatically append on the corresponding values to get the instant visitor pass, where the agent will also work independently in both offline/online for automatic updating of information about the individual consulting the UIDAI server online for the first time and saves the information in the database and offline accessing can be done when the person enter or exit at the security gate for the next time where connectivity is missing. Therefore this measure effectively reduces the resources such as time and cost.

REFERENCES

1. Raghunathan, V.S., S. Dinesh Kumar and G. Thamaraiselvi, 2015. E-Governance service delivery platform – platform to optimize SDLC, Re- Engineering Application Architecture and elimination of process, National Conference On Innovative Computing Techniques, 7(05): 144-149.
2. Zahid Akhtar, 2012. Security of Multimodal Biometric Systems against Spoof Attacks, Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy, pp: 204-209.
3. Wong, W. and N. Memon, 2001. Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification, IEEE transactions on image processing, 10(10): Oct. 2001.
4. Tisse, C.L., L. Torres and M. Robert, 2002. Person Identification Technique Using Human Iris, Proc. of the 15th International Recognition conference on Vision Interface,
5. Sharma Director General R.S. and Mission Director, 2013. Unique Identification Authority of India Aadhaar Creating Identities for 1.2 Billion Indians, uidai. pp: 354-360.
6. Roy, G. and S.M. Musa, 2012. A Simple Model For Biometric Identification Technology Using Fingerprint Scanning, pp: 403-409.

7. Drira, H., B.B. Amor, M. Daoudi and A. Srivastava, 2009. Nasal region contribution in 3D face biometrics using shape analysis framework. Proceedings of the 3rd IAPR/IEEE International Conference on Biometrics, Alghero, Italy, pp: 357-366.
8. Sahoo, Soyuj Kumar; Mahadeva Prasanna, SR, Choubisa, Tarun and Mahadeva Prasanna, 2012 "Multimodal Biometric Person Authentication: A Review, IETE Technical Review 29(1): 54. doi:10.4103/02564602.93139 (inactive 20150104).
9. Brunelli, R. and D. Falavigna, 2014. Person Identification Using Multiple Cues, IEEE Trans. PAMI, 17(10): 955-966.
10. Abdullayeva, F., Imamverdiyev, V. Musayev and J. Wayman, 2008. Analysis of security vulnerabilities in biometrics systems. Proceedings of the Second International Conference on Problems of Cybernetics and Informatics.
11. Thein, H.T., M.M. Sein and S.N. La Aung, 2013. A Reliable technique for personal identification or verification," IEEE International Symposium on Micro-NanoMechatronic and Human Sciense, pp: 265-269.
12. Zhang, D., W.K. Kong, J. You, *et al*. 2003. Online palmprint identification. IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(9): 1041-1050.
13. Jain, A.K., S. Pankanti and R. Bolle, 2012. An Identity-Autentication System Using Fingerprints, Proceedings of the IEEE, 85(9): 1365-1388.
14. Karthik Krishnamurthi, S. Irudaya Mary, B.N. Sumalatha and Adler Pereira, 2015. Fingerprint Based Attendance System International Journal of Advanced Research in Computer and Communication Engineering, 4(3): 29-36.