Improvised Four Level User Authentication Framework using Biometric Recognition for e-Governance Projects in India: A Security Perspective

Ajeet Singh Poonia, Ph.D.
Govt. College of Engineering & Technology, Bikaner, Rajasthan, India

Govind Singh Tanwar
Govt. Engineering College Bikaner, Rajasthan, India

ABSTRACT
e-Governance is the use of internet technology as a platform for exchanging information, providing services and transacting with citizens, businesses, and other arms of government. e-Governance as an administration tool provides a sound strategy to strengthen overall governance. It not only improves accountability, transparency and efficiency of government processes, but also facilitates sustainable and inclusive growth. e-Governance as a societal tool provides a mechanism of direct delivery of public services to the marginal segments of the society in the remotest corners, without having to deal with intermediaries. e-Governance also deals with the sensitive data of governance, so it requires a sound protected, and impenetrable level of security. Along with securing the e-Governance web portal at higher and abstract level, it also requires maintaining the data confidentiality, integrity and availability at user level. Presently the e-Governance web portal in India has issues with the security aspects and is functional using two basic levels of authentication. This paper highlights the problems related with data confidentiality, integrity and availability which are potential reasons for the failure of e-Government Projects in India. Through this paper we intend to provide solution for the user level authentication related to various e-Governance Projects running in India. In the paper, we have also suggested a new security level framework with four layer authentication, synchronised with the unique identification card (Aadhar Card) system. In this context, we have also tried to evaluate the current status of authentication in e-Governance related initiatives in India and future prospects of e-Governance in India.

Keywords
e-Governance, Security Service Authentication, One-Time Password (OTP), Backup, Replica Copy.

1. INTRODUCTION
The concept of e-Governance started with the advent of government websites in the early 1990s. The system of government is fixed, static, hierarchical and regulated; whereas web is dynamic, flat and unregulated [1]. With the development of Information Technology, increasing dependence on the internet as a transaction medium and the development of adequate infrastructure and regulations, government websites soon developed into a highly potential channel for supporting a frontend and back end applications [2].

In India there is uneven progress. Many government departments and states have planned or implemented some form of e-Government initiatives. For example, in Andhra Pradesh and Karnataka there are three to four departments that have been computerized extensively with online delivery of services for a pilot stage of implementation at all their offices in the state[3]. Although few departments that have gone online have demonstrated remarkable improvements in service delivery, but most of these projects have less isolated success stories without structure for scale-up and replication. A recent study on e-Government readiness classified Indian states into four groups, indicating that 18 out of 26 states have made very little progress on e-government [4].

Indian e-Governance consists of the typical authentication process of the user or employees on a web portal for providing information and delivering services. Their advised or purposed authentication process is not working presently and the process is not using the prescribed biometric authentication process [5]. Presently e-Governance web portal works on traditional framework suggested by technologists focusing on encrypted data with old, simple and easily penetrable authentication process. It consists of two levels, Registration / Login and One-time Password (OTP).Currently OTP is more widely used in e-Governance web portal. Though this process provides some security for unique login but as major limitations; as identifying the user with the help of user's mobile number; accessibility of seeds if authentication server is compromised; and it can be broken with man-in-middle attack method. Other limitations of this current framework are: non availability of any backup options if a national level disaster occurs; does not cover all aspects regarding authorization; not general enough to describe fully the security and backup process in a way which will assist the development of new framework techniques [6].

In context of present developed globalization, Indian e-Governance web portal requires the major improvement in authencation process [7]. Hence we try to suggest a new authencation process with the help of Unique Identification Card (UID) known as Aadhar Card system.

2. SUGGESTED NEW CONCEPT OF AUTHENTICATION FOR E-GOVERNANCE IN INDIA

2.1 New Authentication Service Provision Framework
It consists of four different levels for user authentication. User will be uniquely identifies at each and every step in fig. 1: Flow Chart of New Authentication Service Provision. The levels and their working in give below:

Level 0: This is the lowest level of security available and starts the system authentication using username and password. Those users who fill registration form and provide basic information will be provided with the capability of self-registration by which he/she can generate a username/password [8].

Level 1: At Level 1, after matching the username/password combination, the system requests user's Unique Identification Card number (Aadhar number), After entering the user's UID system will generate a background process and match all registration form information with user's UID database. If matching is done successfully then the system will generate SMS-OTP on Mobile, otherwise OTP will not be generated and the system automatically signs-off. At this level system uniquely identifies the user initially[6]. This process is one-time process means system requires user's UID when user signs_up the first time, after that user's UID is stored in the registration database and directly generates the OTP.

Level 2: After successful completion of level 2, the web administrator issues Personal Identification Number (PIN) to the user. This number is 16 Bit long &a combination of alphabet, numeric and special character[9]. Primary purpose of PIN number would be to prove his/her identity through software token (along with PIN). Token would be a digital certificate/digital signature or a smart card or personal identification number (PIN) issued by a higher authority that would be required from the login. Once the PIN is generated, the user will not be able to change this [10].

Level 3: The user will have to prove his/her unique identity with the help of biometrics scan. This is the highest level of authentication validated by user's UID database provided at level 1.The user will be able to access government services and information after they successfully prove their unique identity.

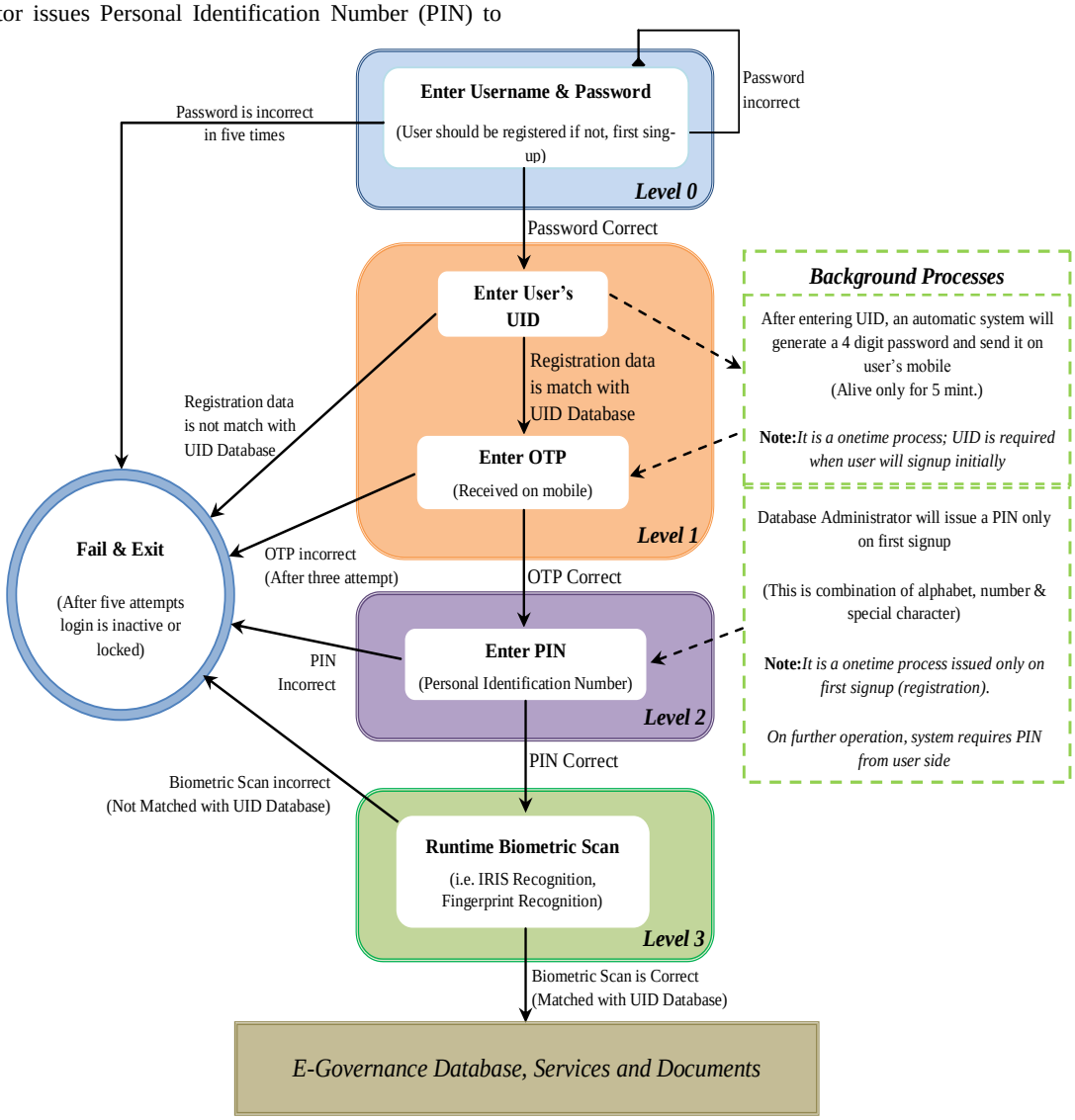

Fig 1.Flow Chart of New Authentication Service Provision

2.2 Backup Provision

Backup is very useful for any system. The present Indian e-Governance system does not consist of any backup, nor is any-purposed or suggested for future implementation in case of a national level disaster [11]. We also suggested a backup framework in this research paper in fig.2: New Suggested Backup Framework for e-Governance. Same is described below:

2.2.1 Multiple Backup's Management

Backup should be saved in different copies; if one copy is crashed or damaged then other copy's data would be used for restoring and saving the data, the copies are stored in different places.

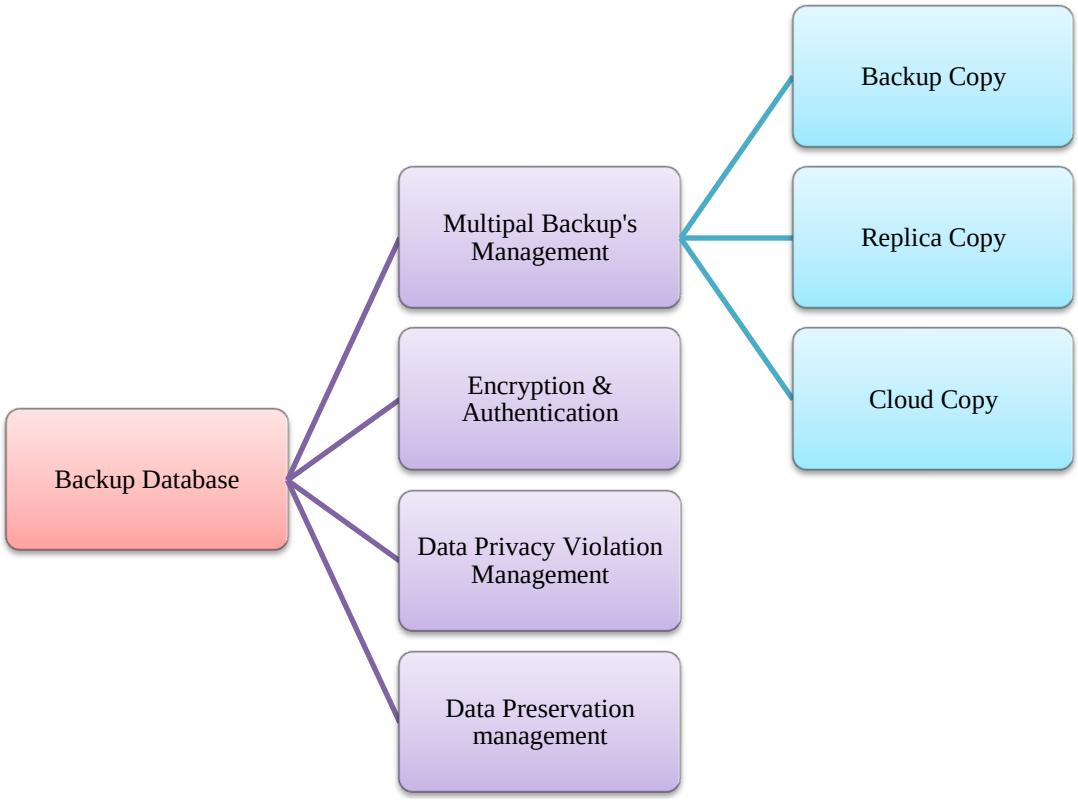

Fig. 2: New Suggested Backup Framework for e-Governance

- *Backup copy* – Refers to a copy of data that may be used to restore the data when original database is crashed or is deleted/erased by any malicious activity. It is stored in another electronic media like hard disk, pen drive, CD/DVD for the historical data or stored with the original database at the same server for automatically restoring the database. It is made in different types: incremental backup, binary backup, encrypted backup, automated database duplication etc.

- *Replica copy* – Refers to making a duplicate database of the original at different location, different network, or in different time zone for the user's availability. A replica is generated at the time of original database creation. In the database management system more than one replica is generated at different locations at the same time. A replica is generated with by the help of triggers. It reduces network traffic because user does not require connecting to the central/main database. Its copy or a part of database as per user requires, when user does any change in the copy. It is automatically done in the original when all replicas are connected with the original database.

- *Cloud copy* – The database should be saved in the cloud. It is classified in two part public cloud and private cloud, government data is assistive data so that it is stored in private cloud and is accessible to the authorized person only. Public cloud is open access means each and every person can easily access the data.

2.2.2 Encryption and Authentication

After taking different form of backup of original database, all the backup copies are stored in encrypted format. All the data is in encrypted format is the responsibility of database administrator (DBA). It uses the present encryption algorithm to encrypt the data and also takes the MD5 for the data. Our system is an automated system firstly it requires administrator's MD5 and calculate the encrypted backup copy MD5 if both are same then the administrator is able to access the backup copy [12]. It's only accessible for DBA or higher authority of Indian government or committee member of e-Governance.

2.2.3 Data Privacy Violation Management

Entities include the use of unique identity number or predefined patterns that are quickly recognized. That is also managed with workflow to key security and reduces individuals'_ information risk.

2.2.4 Data Preservation Management

In preservation, all the backup copies are preserved that were take previously, quarterly in a year. This storage is not for the disaster policy. The media in which these preservation are made, is not available after completion of the process. It is done for archiving the database, archive means that it taken in separate storage media and retained for long periods. Archive is not used actively. This is stored in mainly three different types: XML, text and/or binary documents, plus metadata. The type to be used is not under user control.

3. RESULTS

The suggested work complication is based on current e-Governance system. We advocate more secured authentication process by using biometric recognition for uniquely identify the user. This biometric recognition is based on widely available resource in country (UID/Aadhar Card System).Other important suggestions are advocacy of secured backup database with appropriate authentication and data preservation system.

4. CONCLUSION

During the last few years, many initiatives have been taken by different state governments in India for using IT as a tool in the functioning of e-Governance so as to provide better services to citizens. The greatest shortcoming of security enhancement is the absence of comprehensive law and a structured framework to cope with attack anywhere in the world. The difficulty has exponentially increased due to imbalance in augmented growth of internet & less awareness in security. In this paper we have tried to suggest a generalized framework for government web portal. It can be applied on almost all types of authentication. This also shows the amount of effort that needs to be dedicated to properly authenticate a digital user. Given the current high level of political commitment and largely adequate sources of funding, India is likely to soon emerge as a leader in E-Governance.

5. REFERENCES

[1] Government of India, Department of Administrative Reforms and Public Grievances, "National e-Governance Plan," accessed Apr. 26, 2012, http://arc.gov.in/11threp/ARC_11thReport_Ch7.pdf, 106.

[2] Maheshwari B., Uma Kumar V.K et al. E-Governance Portal Effectiveness: Managerial Considerations for Design and Development. Computer Society of India, 2007: p.1-12.

[3] Sharma S.K., Gupta J.N. Building Blocks of an E-Government: A Framework. 2003, IGL Global. p.34-48.

[4] e-Governance Policy for Modernising government through digital democracy in India, Journal of Information Policy 2 (2012): 183-203.Online ISSN: 2158-3897

[5] Aggarwal S. "UID - Challenges, Applicability and Opportunity". pp-1-8.

[6] Sharma S.S. An E-Government Service Framework. 2006. p.376-378.

[7] Unique identification card project: http://www.UIDAI.gov.in

[8] Ministry of Communication and Information Technology, e-Pramaan: Framework for e-Authentication, Information Technology Editor. 2012, Government Press. p.18.

[9] CIO, H.K.O.o.G., 2008 Digital 21 Strategy – Continuing to build on our strength through technology across the community. 2004, Commerce and Economic Development Bureau: Hong Kong.

[10] IDA, Innovation, Integration and Internationalization – Report by iN2015 Steering Committee. 2006, Information communication Development Authority: Singapore.

[11] Headquarters, I.S., e-Japan Strategy. January 22, 2001 Prime Minister of Japan and His Cabinet.

[12] Headquarters, I.S., e-Japan Strategy II, I. Technology, Editor. 2003: Japan.

6. AUTHORS' PROFILES

Dr. Ajeet S. Poonia was born in Rajasthan, India in 1980. He did his Ph.D from Malviya National Institute of Technology, Jaipur, India in 2013 in Cyber Security Domain. He has 11 years of teaching experience and 07 years of research experience. Presently he is working as an Associate Prof. (Dept of Computer Science & Cyber Security) at College of Engineering & Technology, Bikaner, Rajasthan, India. He has written 03 books, and many research papers at International Journals and conferences. He has organized several programs both at National and International level. He is active member of different societies concern to Computer, IT and Cyber Security domain. He is working as a cyber security consultant and have imparted around 10 training programs to defense personals. His area of interest if Cyber Crime, Cyber Investigations, Cyber Security and Cyber forensics.

Govind S. Tanwar was born in Bikaner, Rajasthan in 1985. He received the B.E. degree from University of Rajasthan, Jaipur, Rajasthan in 2007.

In 2007, he joined the Govt. Engineering College Bikaner as an assistant professor. After that he is doing his M.Tech. From Suresh Gyan Vihar University, Jaipur, Rajasthan in 2013 respectively. Presently he is working as a Assistant Professor in Govt. Engineering College Bikaner, Rajasthan, India. During his teaching tenure he published over 10 research articles in journal and conference in the areas of quantum encryptions, PKI, Data encryption and decryption and image processing. His representative published articles lists as follow: Public Key Technology Introduction Infrastructure (International Journal of Computer Applications, 2010), PKI Encryption Algorithms: A Comparatively Study on QKD, XKMS, KDM (International conference on Computer Engineering and Technology, 2010). In present he is working on Biometric reorganization is using in e-governance of India for improve the system and interwork security. His representative published articles lists as follow: Enhance Security System of E-Governance (International Journal of Engineering Research & Technology, 2013), Biometric Recognition in Implementation in e-Governance in India: A Newer Perspective Era (International Conference on Biometrics Security and Multimedia 2014), etc. Moreover, he was a participant of reviewer in 2010 to presently.