

# **Enhancement of Security System for E-Governance using UID in Context to India**

A

**Dissertation**

*Submitted*

*in partial fulfillment*

*For the award of the Degree of*

***Master of Technology***

***in Department of COMPUTER SCIENCE Engineering***

**(With specialization in Software Engineering)**



## **SUPERVISOR**

Mr. Chitresh Banerjee

Assistant Professor

## **SUBMITTED BY**

Govind Singh Tanwar

Enrol. No.:

SGVU111516336

**Department of Computer Science Engineering**

Suresh Gyan Vihar University

Mahal, Jagatpura, Jaipur

**October -2013**

## **CANDIDATE'S DECLARATION**

I hereby declare that the work, which is being presented in the Dissertation, entitled  
“Enhancement of Security System for E-governance Using UID in Context to India” in

partial fulfillment for the award of Degree of “Master of Technology” in Dept. of Computer Science. Engineering with specialization in Software Engineering **and submitted to the Department of Computer Science Engineering**, Suresh Gyan Vihar University is a record of my own investigations carried under the Guidance of Mr. Chitresh Banerjee, Department of Master of Computer Application.

I have not submitted the matter presented in this Dissertation anywhere for the award of any other Degree.

**(Name and Signature of Candidate)**

Software Engineering

Enrolment No.: SGVU111516336

**Counter Signed by**

Name (s) of Supervisor (s)

Mr. Chitresh Banerjee

## DETAILS OF CANDIDATE, SUPERVISOR (S) AND EXAMINER

**Name of Candidate:** Govind Singh Tanwar **Roll No.** SGVU111516336

**Dept. of Study:** Computer Science Eng.

**Enrolment No.** SGVU111516336

**Thesis Title:** Enhancement of Security System for E-governance Using UID in Context to India

<b>..... Supervisor (s) and Examiners Recommended</b> <b>(with Office Address including Contact Numbers, email ID)</b>		
<b>Supervisor</b>  Mr. Chitresh Banerjee  Assistant Professor  Gyan Vihar University , Jaipur  <a href="mailto:chitreshh@gmail.com">chitreshh@gmail.com</a>		
<b>Examiner (s)</b>		
<b>1</b>	<b>2</b>	<b>3</b>

Programme Coordinator  
Principal

Signature with Date  
Date

Dean /

Signature with

## ACKNOWLEDGEMENT

First of all I would like to thank almighty god for everything I am/have today. There are several individuals who have played such an integral part in assisting me throughout the master program and ultimately, the completion of this dissertation. My heartfelt thanks and appreciation go to the member of my supervisor, Mr. Chitresh Banerjee. Their help, accessibility, and encouragement throughout the dissertation process were greatly appreciated.

Chitresh sir offered open doors and whatever time was necessary to provide advice and the answers to my many questions, and for that I am very grateful. They spent many hours with me, guiding and assisting me throughout the process. He is open door, patient and attentive ear, and wise counsel will forever be appreciated and also gave valuable and timely suggestion not only for academic but for the personal growth too.

Not only the supervisor but also the HOD, Faculty, Staff of Computer Science & Engineering Department and my fellow members of M.Tech has contributed to my effort. Other than my supervisor, I would like to give heartfelt thanks to Dr. Ajeet Singh Poonia who inspired and motivated me a lot to start and go ahead for this research program.

My deepest gratitude goes to my family for their unflagging love and support throughout my life; this dissertation is simply impossible without them. I am indebted to my father Late Shri B.S.Tanwar, for his blessing. I cannot ask for more from my mother Smt. Chandrakanta Tanwar, as she is simply perfect. I have no suitable word that can fully describe her everlasting love to me.

I would like to express my gratitude towards my Brother Dr.G.S.Tanwar, Sister-in-law Smt. Priya Tanwar, Sister Dr.Gayatri Tanwar Gahlot and Brother-in-law Dr.Nitesh Gahlot for their kind co-operation and encouragement which help me in completion of this thesis. I am very grateful for all of them to sacrifices endured, and the patience and tolerance.

And at last my loving niece "Geet", whose smiling face and notorious activities help me to recharge and refresh after the tedious schedule.

Date: 26<sup>th</sup> October 2013

Place: Suresh Gyan Vihar University, Jaipur

**Govind Singh Tanwar**

## **ABSTRACT**

Human life in today's world is surrounded with technology. Technology has left hardly any space for non-technical things. A small change in an individual's life brings

about a change in the society that individual lives. When society is influenced, the security system or the way that society is governed changes for sure. It is a social phenomenon. With the enormous speed of development of technology governance “by the states is also not only governance” but it is turning out to be an “E-governance”. Gradually but certainly, the method and manner of the way the states govern has radically changed because of the advent of the technology.

Even though, the E-governance is replacing the spectrum of governance; in a country like India, there are certain educational, social and cultural issues which affect the progress of E-governance. Even after creating world class Information Technology (IT) units in private sector in India is going with the providing services and transactions online from the point of view of implementing E-governance in public sector. Enhancement of Technology is always giving the power in our hand. It gives the power like paying your bill, ITR, fund transaction, e-money in our hand at any time with secured gateways or secure system. But at the present time nothing is secure. If we used the biometric password for the online transaction, filling ITR, apply passport, Bill payment etc. This type of security system is very much secured. At the present time in India, is not using such type of secured system.

The researcher seeks to discuss the periphery of E-governance with the challenges involved in the techno-legal management, control and new systems like introduction of Unique Identity Cards in India. Law is the constant instrument of social change. Jeremy Bentham gave us the thought of using this instrument of social change for “greatest good of the greatest number”. By implementing E-governance are we experimenting on various social, legal and technical issues that are the question before the present and the generations to come? As of now we can only analyse the question before society and the law.

**Keyword: - E-governance, Unique Identification Card, OTP, SSL, Biometric Recognition**

## LIST OF FIGURES

Figure No.	Title of Figure	Page No.
Figure 2.1	Regional e-government in Asia	7
Figure 2.2	Regional averages in e-government development	8
Figure 2.3	Electronic Service Delivery Modes	10
Figure 2.4	Web portal of Indian government Department of e-governance	12
Figure 2.5	Front-end and Back-end Challenges	20
Figure 2.6	Aadhaar Card on India	23
Figure 3.1	Current E-governance Assurance Framework	31
Figure 3.2	Security/Privacy framework for Unique Identification Card (UID)	35
Figure 3.3	Central UID Database system architecture	37
Figure 3.4	Aadhaar Authentication and Registration System	40
Figure 3.5	Offline/Online Registration in UID System	42
Figure 4.1	Current Authentication service provision for accessing the data from e-governance web portal	43
Figure 4.2	Different Security Technologys	44
Figure 4.3	Statically review of security technology	47
Figure 4.4	Statistical Analysis showing the current to proposed framework in respect of number of authentication level	48
Figure 4.5	Purposed framework for e-Governance security enhancement	49
Figure 4.6	Authentication Service Provision	50
Figure 4.7	Data Flow of Authentication service provision	51
Figure 4.8	E-governance Services	52
Figure 4.9	The e-Parmaan Gateway	54
Figure 4.10	Interconnection of Confidentiality, Integrity & Availability	55
Figure 4.11	Classification of Data Protection System	55
Figure 4.12	Categorisation of Biometric Recognition	56
Figure 4.13	IRIS Recognition System	57
Figure 4.14	Fingerprint Recognition	58
Figure 4.15	Backup and e-Discovery Framework	61

## LIST OF TABLES

Table No.	Table Title	Page No.
Table 2.1	E-government development in south-Eastern Asia	8
Table 2.2	Example Community Configuration Based on Similarity of e-governance profile	9
Table 3.1	Stage of various services that is using UID	41
Table 4.1	Differences between Electronic Signature & Digital Signature	59

## CONTENTS

<b>CANDIDATE DECLARATION .....</b>	<b>II</b>
<b>ACKNOWLEDGEMENT.....</b>	<b>IV</b>
<b>ABSTRACT.....</b>	<b>V</b>
<b>LIST OF FIGURES .....</b>	<b>VI</b>
<b>LIST OF TABLES .....</b>	<b>VII</b>
<b>CONTENTS.....</b>	<b>VIII</b>
<b>CHAPTER 1: INTRODUCTION.....</b>	<b>1</b>
1.1. E-GOVERNANCE	
.....	1
1.2. UNIQUE IDENTIFICATION CARD	
.....	2
1.3. MOTIVATION OF RESEARCH WORK .....	3
1.4. SCOPE OF RESEARCH .....	4
1.5. OBJECTIVES OF RESEARCH .....	5
1.6. ORGANIZATION OF THESIS .....	6
<b>CHAPTER 2: E-GOVERNANCE DEVELOPMENT IN INDIA .....</b>	<b>7</b>
2.1.INTRODUCTION .....	7
2.1.1. E-GOVERNANCE IN ASIA	
.....	7
2.1.2. STRATEGIES AND POLICIES IN ASIA	
.....	8
2.2.E-GOVERNANCE IN INDIA .....	10
2.2.1. SCOPE OF E-GOVERNANCE .....	12
2.2.1.1. GOVERNMENT TO CITIZEN (G2C) .....	12
2.2.1.2. CITIZEN TO GOVERNMENT (C2G) .....	14
2.2.1.3. GOVERNMENT TO GOVERNMENT (G2G) .....	14
2.2.1.4. GOVERNMENT TO BUSINESS (G2B) .....	15



2.2.2. CHALLENGES OF E-GOVERNANCE .....	16
2.2.2.1. FRONT-END CHALLENGES .....	16
2.2.2.2. BACK-END CHALLENGES .....	18
2.2.2.3. CURRENT CHALLENGES OF E-GOVERNANCE IN INDIA ...	20
2.2.3. ADVANTAGE & DISADVANTAGE .....	20
2.3. UNIQUE IDENTIFICATION CARD (UID) .....	22
2.3.1. INTRODUCTION .....	22
2.3.2. WHAT IS UID (UNIQUE IDENTIFICATION) .....	22
2.3.3. LEGAL AMENDMENTS .....	24
2.4. OTHER COUNTRIES .....	24
2.4.1. UNITED STATES .....	24
2.4.2. CANADA .....	24
2.4.3. UNITED KINGDOM .....	25
2.4.4. BRAZIL .....	25
2.4.5. AUSTRALIA .....	25
 <b>CHAPTER 3: LITERATURE REVIEW</b>	
.....	<b>26</b>
3.1. INTRODUCTION .....	26
3.1.1. THE LITERATURE	
.....	26
3.2. E-GOVERNANCE OF INDIA	
.....	26
3.2.1. INFORMATION SECURITY ASSURANCE FRAMEWORK .....	26
3.2.1.1. INFORMATION SECURITY .....	26
3.2.1.1.1. CATEGORIZATION OF INFORMATION SYSTEM	
.....	31

3.2.1.1.2.	SELECTION OF BASELINE SECURITY CONTROLS	
.....		32
3.2.1.1.3.	RISK ASSESSMENT	
.....		32
3.2.1.1.4.	REFINEMENT OF THE SECURITY CONTROLS BASED ON RISK ASSESSMENT	
.....		32
3.2.1.1.5.	IMPLEMENTATION OF THE SECURITY CONTROLS	
...		32
3.2.1.1.6.	MONITORING AND ANALYSIS OF THE EFFECTIVENESS OF THE SECURITY CONTROLS	
.....		32
3.2.2.	POLICY OF E-GOVERNANCE OF INDIA .....	33
3.3.	UNIQUE IDENTIFICATION CARD (UID) .....	33
3.3.1.	LEGAL FRAMEWORK .....	33
3.3.1.1.	PROTECTION PRIVACY AND CONFIDENTIALITY	
.....		34
3.3.1.2.	DATA SECURITY AND FRAUD	
.....		34
3.3.1.2.1.	PROTECTING PERSONAL INFORMATION OF RESIDENTS	
3.3.1.3.	TECHNOLOGY ARCHITECTURE OF UIDAI .....	36
3.3.1.3.1.	SYSTEM ARCHITECTURE	
.....		36
3.1.3.1.1.	THE UID SERVER	
.....		36

3.1.3.1.2. THE BIOMETRIC SUBSYSTEM	36
3.1.3.1.3. THE ENROLMENT CLIENT	37
3.1.3.1.4. THE NETWORK	37
3.1.3.1.5. THE SECURITY DESIGN	37
3.3.2. AADHAAR AUTHENTICATION AND CURRENT FRAMEWORK	38
3.3.2.1. DEMOGRAPHIC MATCHING	39
3.3.2.2. BIOMETRIC MATCHING	40
3.3.2.3. MATCHING USING ANY OTHER FACTORS SUCH AS ONE-TIME-PASSWORD (OTP)	40
3.3.2.4. ISSUING THE UID NUMBER	41
3.3.2.4.1. TYPE OF AUTHENTICATION	42
3.4. RESEARCH GAP	42
<b>CHAPTER 4: DEVELOPMENT OF HIGH LEVEL SECURITY SYSTEM FOR INDIA</b>	
4.1. CRITICAL ANALYSIS OF EXISTING MODEL	44
4.2. CRITICAL REVIEW OF SECURITY TECHNOLOGIES	44
4.3. DRAWBACKS OF EXISTING FRAMEWORK	48
4.4. DEVELOPMENT OF HIGH LEVEL SECURITY SYSTEM FOR E-GOVERNANCE OF INDIA	49
4.4.1. REGISTRATION & AUTHENTICATION	50

4.4.1.1.	AUTHENTICATION SERVICE PROVISION .....	51
4.4.2.	E-GOVERNANCE SERVICES .....	53
4.4.2.1.	SECURE SITE SERVICE .....	53
4.4.2.1.1.	SECURE SOCKET LAYER (SSL)	
	.....	53
4.4.2.1.2.	E-PARMAAN GATEWAY	
	.....	54
4.4.2.2.	DATA CONFIDENTIALITY & PROTECTION	
	.....	55
4.4.2.2.1.	BIOMETRIC RECOGNITION .....	57
4.4.2.2.2.	DIGITAL SIGNATURE PROCESS .....	59
4.4.2.2.2.1.	LEGAL VALIDITY .....	60
4.4.2.3.	BACKUP AND E-DISCOVERY .....	61
4.4.2.3.1.	BACKUP .....	62
4.4.2.3.1.1.	MULTIPLE BACKUP'S MANAGEMENT .....	62
4.4.2.3.1.1.1.	BACKUP COPY	
	.....	62
4.4.2.3.1.1.2.	REPLICA COPY .....	63
4.4.2.3.1.1.3.	CLOUD COPY .....	63
4.4.2.3.1.2.	DATA PRESERVATION MANAGEMENT	
	.....	63
4.4.2.3.1.3.	DATA PRIVACY VIOLATION MANAGEMENT .....	64
4.4.2.3.1.4.	ENCRYPTION & AUTHENTICATION	
	.....	64
4.4.2.3.2.	E-DISCOVERY .....	64
4.4.2.3.2.1.	RECORD DECLARATION .....	64

4.4.2.3.2.2.	CLASSIFICATION & RETENTION	64
.....		
4.4.2.3.2.3.	INTELLIGENT NAVIGATION .....	64
4.4.2.3.2.4.	COMPLIANCE WORKFLOW .....	65
<b>CHAPTER 5: RESULT AND CONCLUDING REMARKS</b>		
.....		<b>66</b>
5.1. RESEARCH FINDINGS .....		66
5.2. LIMITATIONS OF THE RESEARCH .....		67
5.3. CONCLUSION		
.....		67
<b>ANNEXURE – I</b>		
<b>ANNEXURE – II</b>		
<b>REFERENCES</b>		
<b>PUBLISHED PAPER</b>		
<b>PLAGIARISM PERCENTAGE REPORT</b>		

## CHAPTER 1

### INTRODUCTION

#### 1.1 E-Governance

The information and communication technology (ICT) industry has got a very good expansion in the last two decades. India became a global leader in the ICT sector on the basis of its advantages of talent pool, lower operational cost and the innovative remote delivery model. Principally, ICT has two sectors, first information technology (IT) and second Communication. In the world's other country just behavior with India as a bureaucratic economy country but they don't know the India is leading IT market in the whole globe, Indian IT sector has played an important role in changing of the innovative entrepreneurs. The major growth drivers in this Indian sector are online

retailing, cloud computing, e-commerce and E-governance.

The new revolutionary emergence in Information and communications Technology (ICT) has brought a novel plan for governance on the ground of possibility. E-Governance makes comprehensive decisional processes and the use of Information and communications Technology (ICT) for proper contribution of Indian citizen in public affairs, as they are important participants in this e-Governance system. The aims of implementing e-Governance are to improve governance processes and outcomes with a proper vision to get better delivery of public services to citizens. As some authors have described e-Governance as the e-business, it seems suitable as both e-Governance and e-business use similar hardware, technologies and infrastructure. Conversely the market definitions are widely anonymous thus validating e-Governance as a separate area of research. However, there are various definitions of e-governance; the aims of governments are indisputable: maintaining security, administering proper justice, providing the institutional infrastructure to the national economy and ensuring that vital social capital is augmented through improvements in health and education.

A broad definition of e-Governance proposes following changes of government in two related aspects:

- 1) Renovation of business of governance i.e. decreasing costs, improving service delivery and renewing processes;
- 2) Follow-up and feedback of the functions and processes of democracy itself.

The emerging results are diminished costs, lesser corruption, improved transparency, new revenue generation and more facilities for the citizens.

India as a developing nation still lacks an E-governance enabling legal framework. The Information Technology Act, 2000 provides for the legal recognition to electronic communications, electronic transactions and storage of information and data in electronic form for subsequent reference. It also enables certain government agencies to facilitate filing; submission of forms related some specific processes, e.g. Income Tax Department, Banking Processes, etc. The Information Technology Act, 2000 was amended comprehensively in 2006 and 2008 which has made adequate effect in transforming some areas of governance into e-governance. But this is just a beginning. The real transformation from State to Welfare State and Welfare State to Modern State with better governance will become Modern State with E-governance.

Efficient e-governance is a novel, inventive and more transparent method to deliver

government services to citizens and exchange information with them in a more convenient, facilitate and transparent way with saving time and money.

## **1.2 Unique Identification Card (UID)**

To all are the Indian citizen allocating unique identification number its callas the Aadhaar number. It is issued by the Unique Identification Authority of India (UIDAI). With the Aadhaar enrolment already taking place at many locations across the country, the downstream services and applications of the Unique Identification (Aadhaar) number shall need to be formulated and operationalized. For the online authentication UIDAI proposes use of demographic and biometric data of citizens. The UID (Aadhaar) Number, is a matchless identity for the entire citizen, this is allocated to all of them it means that every citizen have a matchless separate identity that is issued by public agencies or private agencies at the behalf of the government.

The purposes of Authentication are following:

- (1) To allow Aadhaar-holders to prove identity and
- (2) For service providers to confirm the resident's identity claim for services delivery and give access to detriments. Aadhaar Authentication shall make life simpler to the resident as it is meant to be a convenient system to prove one's identity without having to provide identity proof documents whenever a resident seeks a service.

The mechanism of Aadhaar Authentication is to submit the Aadhaar number along with the Aadhaar holder's personal identity data to the Central Identities Data Repository (CIDR) for matching. Then CIDR authenticates the genuineness on the basis of the submitted database of match with the Aadhaar holder's identity information available with it. The UIDAI verifies the proof of identity or the information provided by the resident based on the data available in the CIDR at the time of Authentication. To protect resident's privacy, Aadhaar authentication service responds only with a "yes/no" and no Personal Identity Information (PII) is revealed.

The 'Aadhaar Authentication Framework' details the Authentication types offered by UIDAI as Demographic Matching and/or Biometric/ OTP Matching, by which citizens can authenticate themselves using the system in several ways with the necessity of submission of the Aadhaar Number with respect of 1:1 matching operation.

## **1.3 Motivation for research work**

E-governance (Digital Governance) is an upcoming and is talk of the town in every field of the society/system. Not only the technical but also the common man of the system/society has begun to understand its importance. Theoretically and practically this is a new system/subject for researchers and is growing exponentially. Lot of work has been done and endless has to be go because the invention or up gradation of new technology leads to the technical support i.e. the digital or we can say the cyber government or e-government. This is because every day a new technique project is being developed for doing the e-government and many times we are not having the proper method/model/technique to tackle that newly e-governance project.

The available method/model/technique mainly concentrates on part of the process (dealing with gathering, analyzing and presenting documents) and they do not explicitly identify the information flows in the process with secure manner. Many current methods are simply too technology specific. Also the prosecution and conviction of e-governance is completely based on paper work or less security not based on the standard models developed during last two decades. The largest gap in most of the presented days is, no attention has been paid on the delicate security enhancement and also on data acquisition process.

Adequately address the problem of lack of security services in e-government maturity models, in relation to the goal of this research work. This section briefly presents main problem of present e-governance security loopholes for IT security terms: security risks, security threats and security vulnerabilities in relation to e-government services.

**Security risk** refers to the potential that given threats would exploit vulnerabilities of e-government systems, and consequently cause harm to the organization information assets. Security risks affect confidentiality, integrity and availability (CIA) of e-government information assets while being processed, transmitted and stored across e-government domains.

**Security threats** refer to any situation or condition it refers to very harmful for all organizations critical assets, through un-authorized access, destruction, disclosure, or modification of information assets. Security threats exploit specific vulnerabilities within e-government systems and applications;

**Security vulnerability** refers to flaws or weaknesses in system security procedures, design, implementation, and/or internal controls that could be exploited by threat sources.



Reducing any of the three elements, security threats, security vulnerabilities and impact, could result into a significant reduction of security risks.

#### **1.4 Scope of the Research**

Overall it can be concluded that this research will help to develop a security model for a least e-governance society and readiness to fight against the existing and new generation security model i.e. the technology driven security by adopting various methods, tools, techniques of Information Technology to our administration i.e. e-governance officials and a common man to compete the world and to be aware from the latest technology/projects through the IT for the present and upcoming scenario. Briefly we can summarize the scope of the research as following:

- A. It will be helpful to solve the technology enabled security, which will bring transparency in the system.
- B. It will reduce the time of monitoring, capturing, identifying the every person information in India.
- C. It is a general model with respect to technology and follows the steps, that an actual security implementation would take place.
- D. It will provide a reference, a technique, a procedure, a method, a framework, an environment independent of any particular type of security enhancement for any system or any organization, for supporting the work of any information.
- E. It can be used in a practical way to identify opportunities for the development and operation of technology/methodology to support the work of information.
- F. It can be used to help to develop or implement and apply methodologies to exiting two different projects, as they emerge and become the subject of information's.
- G. For the non-technical viewer is easy to understand and implemented, so it will act as generalized approach
- H. This will allow tools to be specified and developed, dealing with case management, examination of system, and the controlled dissemination of information.

#### **1.5 Objective of the Research**

Other than scope defined above, there also few objectives behind this research, which are discussed below:-

- A. To implement a more security system to respond the e-governance information incidents to bring the faith and confidence to fight against the incorrect information.
- B. To help in assessing the potential e-governance information.
- C. To improve security management in the public and private sectors.
- D. To improve regulatory tools and mechanisms to minimize incorrect information regarding the citizens of India.
- E. To improve and facilitate the interface to Indian citizens information to our government, if involved;
- F. To proposed Unique Identification Cards system is complete with required legal framework, is there modification of legislations in India.
- G. To proposed exiting implementation of Unique Identification Card System as the new security mechanism for successful implementation of E-governance in India.
- H. The current legal framework in the form of Information Technology Act, 2000 is adequate for successful implementation of E-governance and the emerging information and communication technologies in India.

## **1.6 Organization of the thesis**

Chapter 2 covers about overview of E-governance, implementation of e-governance in India and also the issues, challenges in India for successful implementation of E-governance and unique identification card (UID) project with current framework. Chapter 3 covers review of literature on E-governance and unique identification card (UID) project and its workability, legal framework, technologies and current mechanism utilised for it and justifications for use Unique Identification Cards in India. Research Gap has been discussed here, after the literature review. Chapter 4 deals with the final proposed framework of e-governance with biometric password dictation system using Unique Identification Card. Chapter 5 Result and the Conclusions of the researcher about the efficacy of regulations relating to the information and communication technologies and e-governance in India.

## E-GOVERNANCE DEVELOPMENT IN INDIA

### 2.1 Introduction

#### 2.1.1 E-government in Asia

Most Asia-Pacific countries have gone beyond questioning the potential of information and communications technology (ICT) for social and economic development and have accorded ICT an important place in their policy and planning agendas. When properly deployed, ICTs are seen to play an important role in stimulating economic growth and development by providing new and more efficient methods of production, bringing previously unattainable markets within the reach of the poor, improving the delivery of government services, and facilitating the management and transfer of knowledge [1].

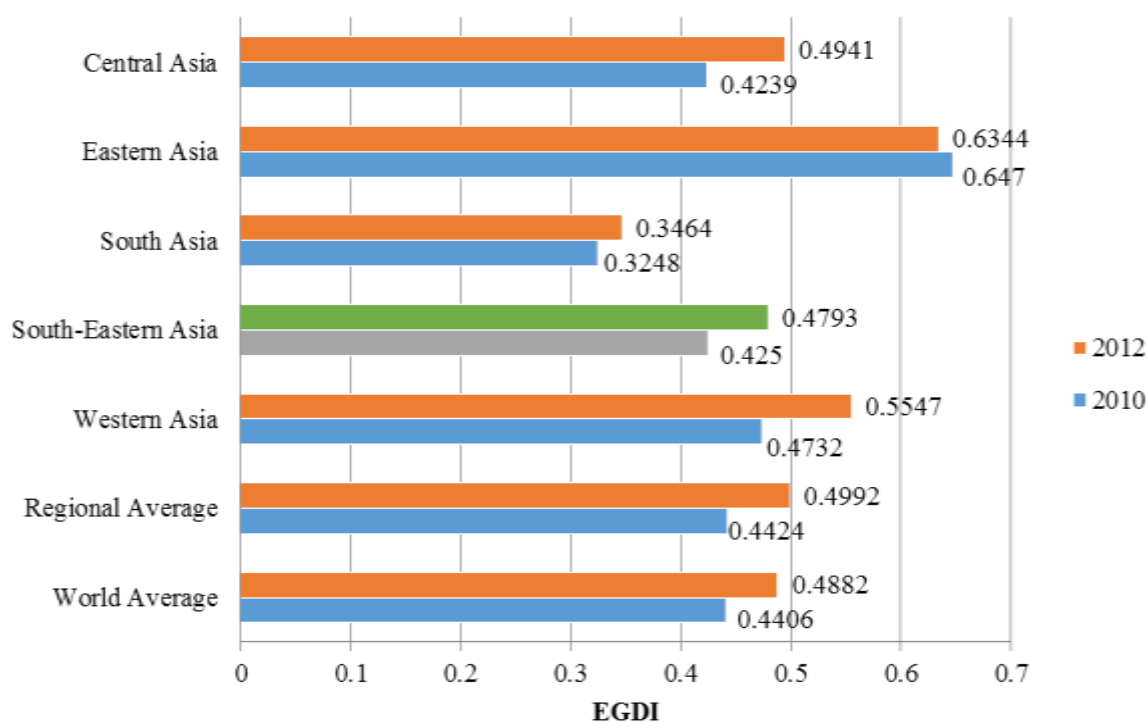


Figure 2.1: Regional e-government in Asia

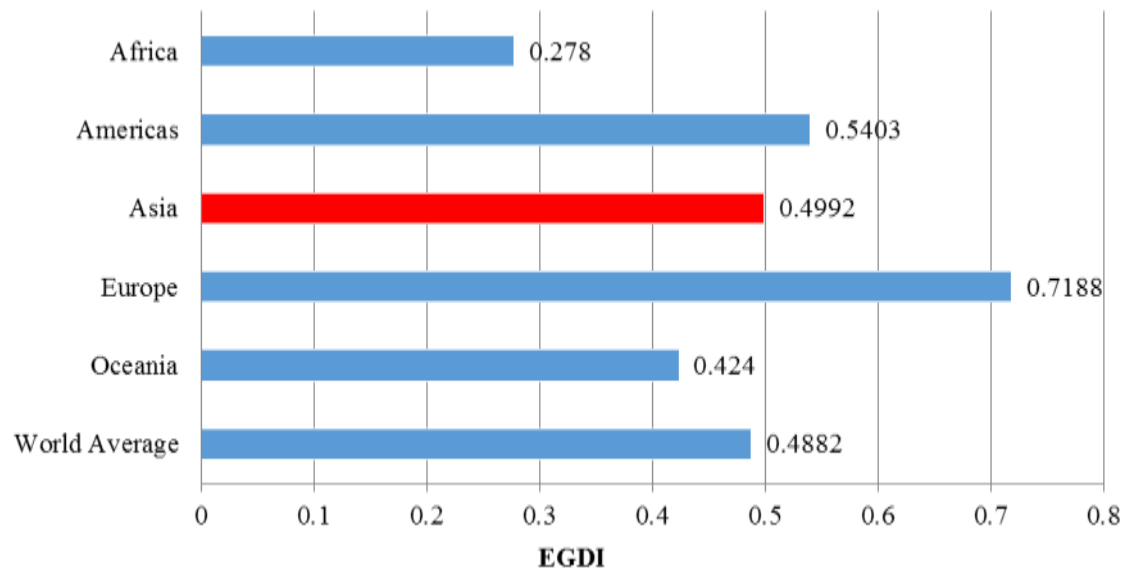


Figure 2.2: Regional averages in e-government development

Country	E-gov. development index		World e-gov. development ranking	
	2012	2010	2012	2010
Maldives	0.4994	0.4392	95	92
Iran (Islamic Republic of)	0.4876	0.4234	100	102
Sri Lanka	0.4357	0.3995	115	111
<b>India</b>	<b>0.3829</b>	<b>0.3567</b>	<b>125</b>	<b>119</b>
Bangladesh	0.2991	0.3028	150	134
Bhutan	0.2942	0.2598	152	152
Pakistan	0.2823	0.2755	156	146
Nepal	0.2664	0.2568	164	153
Afghanistan	0.1701	0.2098	184	168
<b>Sub Regional Average</b>	<b>0.3464</b>	<b>0.3248</b>		
<b>World Average</b>	<b>0.4883</b>	<b>0.4406</b>		

Table 2.1: E-government development in south-Eastern Asia

### 2.1.2 Strategies and Policies in Asia

We identify examples of e-governance strategies employed by the leading countries and economies in Asia – Hong Kong [2-3], Singapore [4], Japan [5-6], Korea [7] and India [8]. E-governance strategies are usually specified as part of an overall ICT or Knowledge Society Strategy. We rely on the knowledge base described in [9]

to extract and consolidate e-governance strategies, IT infrastructure strategies and digital divide strategies spanning the four economies, which include:

- Strengthening linkage between informatization and public administration reform [10].
- Better integrating the structures of government [11].
- Encouraging greater electronic participation in policy process through various channels (e.g. Web 2.0) enveloping mobile government infrastructure [12].
- Extensive use of public consultation and feedback, particularly in policy matters [10].
- Building strategic partnership with the private sector and the civil society [10].
- Providing electronic services for the private sector [11]

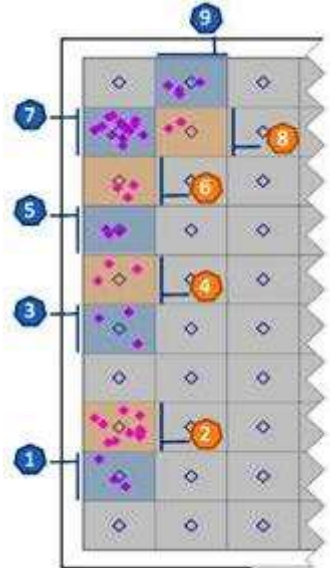
Community	Country Members	Spatial Ordering of Groups
<b>Community 1</b>	Kuwait, Pakistan, Qatar	
<b>Community 2</b>	Bahrain, Cyprus, Israel, Japan, Malaysia, Philippines, Republic of Korea, Singapore, Thailand, Turkey, United Arab Emirates	
<b>Community 3</b>	China, Jordan, Lebanon	
<b>Community 4</b>	Brunei Darussalam, Mongolia, Saudi Arabia	
<b>Community 5</b>	Kazakhstan, Maldives, Vietnam	
<b>Community 6</b>	India, Kyrgyzstan, Sri Lanka	
<b>Community 7</b>	Afghanistan, Armenia, Bangladesh, Cambodia, Democratic People's Republic of Korea, Indonesia, Iraq, Lao People's Democratic Republic, Myanmar, Oman, Syrian Arab Republic, Tajikistan, Timor-Leste, Turkmenistan and Yemen	
<b>Community 8</b>	Azerbaijan, Georgia	
<b>Community 9</b>	Bhutan, Iran, Nepal, Uzbekistan	

Table 2.2: Example Community Configuration Based on Similarity of e-governance profile [10]

Figure 2.3: explores various building blocks/stages in the development of alternate of electronic delivery of services

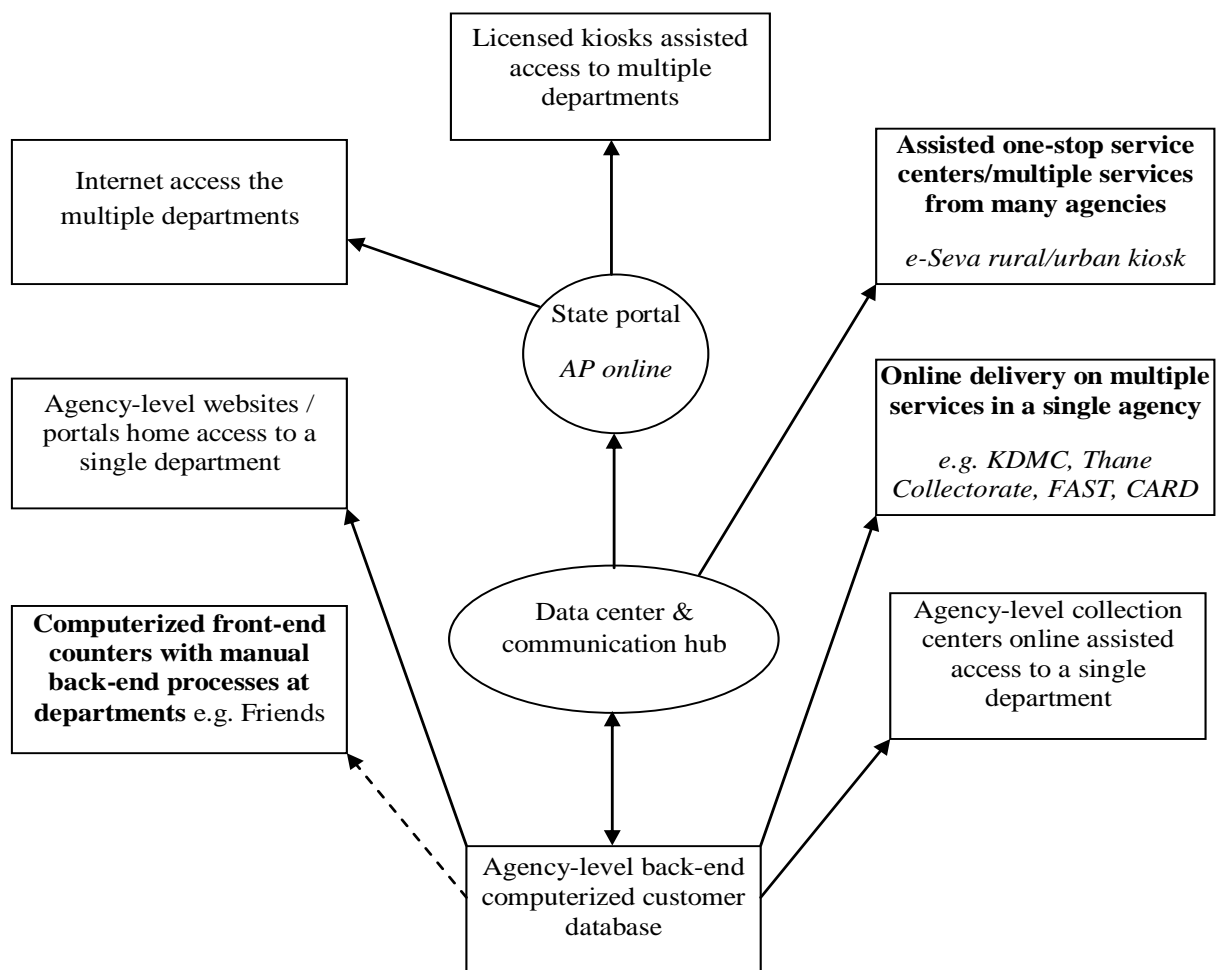


Figure 2.3: Electronic Service Delivery Modes

## 2.2 E-governance in India

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 computerized extensively with online delivery of services at all their offices in the state. In five to six departments, electronic delivery of services is at a pilot stage of implementation. In most of the remaining 50 departments websites have been created but there is no move to offer online services. Although the few departments that have gone online have demonstrated remarkable improvements in service delivery, most of these projects remain relatively 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 [12].

For the development of e-governance, Indian government is developed the new

concept Single Window Cell (SWC) for decrease the corruption. So as per the resultant firstly the Single Window Cell (SWC) is implemented for metropolitan water supply & sewerage in Hyderabad. Before the making of Single Window Cell (SWC) around 120 section offices with the 14 other staff has been worked for payments but after the development of Single Window Cell (SWC) all the application record is maintained in the computer and the information is centralized and publicly open for know the status of application, resultant the official's corruptions are reduced. All the staff members have a individual computer terminals so all of them is motivate to give better services and offices seem like modern offices. The changes are coverage by the social and national media so that the staff members and other offices are motivated and want to implement the system at our [13].

In addition to the national portal, the Government has also developed an India Development Gateway. The Single Window concept is developed by “the National portal of India for access the information and services; the basic purpose is that to reach the rural communities of India with the specific objective. It classified information is use in ICT tools for development escorting and sharing the knowledge” [14]. A variant of the National Portal, but targeted towards a specific group of people, this site contains specific topics aimed at the rural poor: agriculture, rural energy, etc., and features forum discussions and an “ask an expert” section. Making it available in English and in eight local dialects, the government’s main objective is to stimulate women, the poor, and people in the remote rural areas to use technology to their own advantage [10].



## 2.2.1 Scope of E-Governance

Governance is the concept or environment for flow the information form various ways, which are: Government and Citizens, Government and Businesses and Government and Government. E-governance concept is flow all these:

- A. Government to Citizen (G2C)
- B. Citizen to Government (C2G)
- C. Government to Government (G2G)
- D. Government to Business (G2B)

### 2.2.1.1 Government to Citizen

First basic concept for e-governance is government to citizen. In present time, this relationship is starting with the birth of a new citizen and just like end with the death, so between the death and birth the government deals with many features of the citizen's life [15]. Citizen during his/her life made different type of transaction with the government like: starting with birth certificate, marriage certificate, divorce and death certification.

Several services like medical facilities, Post office facilities, Electricity, Telecommunication, Transportation, Education and Banking services are provide by the government at behalf of the Government to Citizen (G2C) relationship. During this government also provide special services like ID card (Voter Card, PAN card etc), Passports, several certificate, Licensing etc.

- a) **E-Citizenship** – Information and communication technology (ICT) develop several facility for citizen in the form of e-citizen. Information and communication technology (ICT) give the more advantage to citizen like transfer the amount form every where, citizen's have a power to renew over documents is Passport, Identity card, Election Card, Ration cards etc. Here it is required a virtual identity to create for access the online services provided by the government. So that citizen database is also maintained by the government.
- b) **E-Registration** – For the purpose of tendering the Information and communication technology (ICT) has been developed a new concept e-registration, during these all the contractor should be register him self, the main benefit for e-registration is no need to extra effort to make the database of all contractor and various contracts information is automatically saved in database. The main advantage of e-



registration to reduced the paperwork and made the record correctly with any duplication.

- c) **E-Transportation** – Information and communication technology (ICT) give one more advantage to citizen is e-transportation, means that the citizen pre-book transport before the date of journey for comfort. Road, Railways and Air all they are online for:
  - i. Current situation of vehicle, rail and air bus
  - ii. Pre-booking and cancellation of tickets
  - iii. Driving licenses renewal and new issued and made a online payment
  - iv. New vehicle and/or renewal old vehicle registration with made a online payment
  - v. Vehicles transfer from one state to another state
- d) **E-Health** – All the hospital should be attached in for plan of e-health. This is the revolutionary change made by Information and communication technology (ICT) for the citizen. In e-health system maintain the local pharmacy database and also make the patient database with the all description.
- e) **E-Education** – Major changes made in education for creating the e-education system developed by Information and communication technology (ICT) India. Resultant distance learning courses will be going to successful. This system help to those student's they are not able to going to school, also the classroom are distant with the help of internet.
- f) **E-Help** – Information and communication technology (ICT) provided the help in disaster and crisis. Such that through e-help they should pre informed the government agencies to the disaster so that they are prepared and make the plan for save the maximum citizen.
- g) **E-Taxation** – One another advantage given by Information and communication technology (ICT) of India is e-tax. Citizen pays our tax online and this also gives the due alerts of tax. This facility give and also help for making the fast online transact.

#### **2.2.1.2 Citizen to Government**

E-governance make the one of another relationship is citizen to government just like another. In Citizen to government relationship occur campaigning, e-voting for democracy and feedback of government.

- a) **E-Democracy** – This is the best way to implanting the democracy. This is reduced the time of citizen and government both, also reduced the cost for implementing the voting and also reduced the paperwork and early declared the result with accuracy and stop the volition during the voting [16]. In which also take the public opinion, feedback about the government and also make the good government.
- b) **E-Feedback** – Information and communication technology (ICT) developed e-feedback for citizen. In this service citizen directly give the feedback to the government. This emerging concept is reduced the lobbying. Use of E-feedback can also made an online debate for the government services.

### 2.2.1.3 Government to Government

After G2C and C2G relationship, government will require a central to state government relationship. This concept is implementation in Government to Government relationship, in these including government departments two or more then two.

- a) **E-administration** – Information and communication technology (ICT) has develop new functioning of the on out side and on inside to government. This functioning can reduce the communication gap between the governments department and government. It also reduces the time and also save the unnecessary paperwork[16]. It also takes transparency and honesty in the government department's administration.
- b) **E-police** – E-police concept is more different form Cyber-Police. E-police does not required the trained electronic or computer person for stopping the electronic crime. Means in which provided all the data regarding the police and criminal at internet so these data play a major role in case investigation. With the help of e-police also reduced the reaction time against the crime or notorious activity, helping of “e” also reduced the paperwork and save the government's money.
- c) **E-courts** – Information and communication technology (ICT) developed a very immerging concept E-courts. In this concept all the judicial processing is online means that the court hearing date, discussion, warrants and judgments and decrees all are available online.

### 2.2.1.4 Government to Business

- a) **E-Taxation** – Information and communication technology (ICT) through this application help to bank for crosscheck the frauds and deficit in payment because the taxes, duties and dues will be made easy for paying online for the major sector corporate [21]. It also reduced the time and cost and we all know the also reduced the paperwork and easy to maintain all the records in the electronic format.
- b) **E-Licensing** – Information and communication technology (ICT) enable all type of licenses online. If a new company is launch and it require the license and many other registrations, all these are made online and reduced the time, paperwork and human efficiency. This is very easy to maintain and also reminds or notify company before expiry date of registration.
- c) **E-Tendering** – E-Tendering give the more prospects to business. The entire tender's information goes online and also shows the current status of tender with the full contractor information. With the help of this application it became easy to maintain all the data of contractor and tenders [17]. Also reduced the time and cost with paperwork and also reduced the human efficiency and make the transparency in tender allotment.

### **2.2.2 Challenges in context to India**

There are large numbers of potential barriers in the implementation of e-Governance. Some hindrance in the path of implementation, like security, unequal access to the computer technology by the citizen, high initial cost for setting up the e government solutions and resistance to change. Challenges identified as trust, resistance to change, digital divide, cost and privacy and security concerns. Although the government has come up with several initiatives to facilitate the access to public services, the desired outcomes are yet to be fully realised. This can be largely attributed to various front-end and back-end challenges that the Government countries to face.

Two major categories of challenges of e-Governance in context to India are:

1. Front-end challenges
2. Back-end challenges

#### **2.2.2.1 Front-end Challenges are:**

##### **2.2.2.1.1. Low penetration of ICT and Limited access to information**

Low internet penetration and digital literacy is likely to weaken the potential of the initiatives taken by the Government. Rural people often complain that there is lack of

access to information about government programmes and services. There is a desire to learn to access information and enjoy their right to information. However, proliferation of computer and computer education is very low in rural areas. The internet penetration has still not reached the desired values. Rural India has 38 million internet users and 31 million active internet users. The internet users are rapidly growth in 2.6% to 4.6% in the rural environment. In this respect also growth in the active user form 2.13% to 3.7% from 2010 to 2012 which will not impressive as compared to rural growth [18].

#### **2.2.2.1.2. Lack of Awareness**

Common man in the country is unaware of the benefits and potential of ICT in his day to day life. The benefits of e-Governance are generally unknown. There is a tremendous need to update citizens of their rights and the services that are being offered to them [19]. Citizens are not aware of their legal right to information or in some cases are reluctant to assert it.

- A massive awareness and communication strategy is required to be launched to educate people about what ICT in general and NeGP in particular can do to improve their lives as well as empower them.
- The second set of audience that needs to be addressed are the stakeholders within the Government structure – politicians, policy makers, directors, secretaries, patwaris, tehsildars and circle officers. A special awareness campaign targeting the group would also be needed.
- The third set of audience is the industry – Central Statistical Organisations (CSOs) and Non-Governmental Organisations (NGOs) – who will help create awareness at local levels and who will research, study and generate findings that can potentially be used to improve projects and their impacts.

#### **2.2.2.1.3. Need for Building Capacity**

India has a very large pool of highly skilled IT professional in high scientific manpower. However, these developments have largely been confined to the urban areas with the exception of a few rural initiatives in some states. There is an urgent need to address the digital divide in the county in an integrated and holistic manner. Government needs to build or strengthen existing institutions to impart IT skills in rural areas [20]. There is also a lack of personnel with appropriate background and aptitude within government framework to handle the programme. In such low capacity

environments, record management and statistics generation may be insufficient to support access to information. Each of these gaps needs to be addressed adequately.

#### **2.2.2.1.4. Trust**

Chopra and Wallace (2003) suggest that an integrated definition of trust recognises the union of three elements: a trustee to whom trust is directed, confidence that the trust will be upheld, and a willingness to act on that confidence, as follows: “Trust is the willingness to rely on a specific other, based on confidence that one’s trust will lead to positive outcomes” [21].

#### **2.2.2.1.5. Cost**

Cost is one of the most important prohibiting factor that comes in the path of e-governance implementation particularly in the developing countries like India where most of the people living below the poverty line. Elected officers and politician don’t seem to be interested in implementing e-governance. Its return is not visible in the near future. In 2004, the United Kingdom and Singapore respectively spent 1 percent and 0.8 percent of their gross domestic product (GDP) on e-government. India is spending 3 percent of GDP [22].

### **2.2.2.2 Back-end Challenges**

#### **2.2.2.2.1. Lack of interoperability**

Interoperability is one of the biggest challenges faced by the government. There is a lack of consistency in terminologies and methodologies employed by different authorities. Different units, technology, applications may be used for measuring data or same term maybe used with different meaning in different departments. Many government departments have no standards policy [18]. Thus, while creating applications they do not take into considerations the issue of standards or interoperability.

There are thus many components to system non-interoperability,

- Lack of transparency and inter-departmental coordination in data collection.
- Not being able to follow good internal record-keeping practices.
- Missing interconnections between datasets by different departments and cross-verification

- Bottlenecks in web publishing, especially due to not using content management systems and centralising web publishing authority within a department.

#### **2.2.2.2.2. Resistance to Change**

The employees in government ministries/departments, particularly at the state and the local level, lack awareness about the significances of open governance public as well as to themselves. As such, the employees are resistant to any changes in the way of working or in embracing technology. The Government, therefore, needs to organise change management workshops as well as functional trainings to bring about a change in the mindset and enhance skills in the mindset and enhance skills of employees at various levels [18].

#### **2.2.2.2.3. Data Unreliability**

The accuracy of the information is not guaranteed by the government. There is lack of incentives for the government agents to provide quality information as well as lack of civil society accountability programmes checking government data for accuracy [23]. These reliability issues have been faced by most of the citizens and opaque methodologies used for data collection makes it difficult to assess the quality of information.

#### **2.2.2.2.4. Cost of information**

With the increasing awareness enabled by RTI, open data and e-Governance initiatives, there is an increase in overall cost of delivering information to its citizens [24]. Therefore, there is a need for continuous funding of such initiatives through government or private sector. Since most government data was not initially opened, they are not in machine readable format.

#### **2.2.2.2.5. Privacy & Security**

Privacy and maintenance of anonymity wherever required is another challenge. Whenever a citizen gets into any transaction with a government agency, he/she shares personal information, which can be subject to misuse through hacking, phishing and spamming. Like western counterparts, an increasing number of people are now becoming aware and concerned about their privacy. Thus, the citizens need to be ensured that the information flow would pass through reliable channels and seamless network. There will be three basic levels of access exists for e-government stakeholders: no access to a Web service; limited access to a Web-service or full-access to a Web service, however when personal sensitive data exists the formation of

the security access policy is a much more complex process with legal consideration [25]. A lack of clear security standards and protocols can limit the development of projects that contain sensitive information such as income, medical history.

#### 2.2.2.2.6. Digital Divide

The digital divide refers to the separation that exists between individuals, communities, and businesses that have access to information technology and those that do not have such access [26]. Social, economic, infrastructural and ethno-linguistic indicators provide explanations for the presence of the digital divide [27]. Economic poverty is closely related to limited information technology resources. Economic poverty is not the only cause of digital divide. It can also be caused by the lack of awareness among the people. Even some of the economic stable people don't know about the scope of e-governance [28]. Awareness can only help to bring users to that service delivery channel once.



Figure 2.5: Front-end and Back-end Challenges

#### 2.2.2.3 Current Challenges of e-Governance in India

- Lack of effective project management tools and methods.
- The knowledge of project management concepts is very low in Government officials forming part of the e-Governance team.
- During the project initiation, the baseline data is not captured which is useful for bench marking of activities.

- No control of central IT agencies during project execution. The decision making process is generally left to individual line ministries and departments since funding comes from them.
- No monitoring of Cost and Schedule at project checkpoints.

### 2.2.3 Advantages

Following are the various advantages of E-Governance

**2.2.3.1 Speed** – Growth in Mobile, Telephone, Internet have reduced the time of communication between citizens because the technology always make and give the better opportunity.

**2.2.3.2 Cost Reduction** – Paper work is became an old fashion work. This is the time for doing electronically because it save the paperwork and it also reduced the cost. Most of government departments spend lot of amount on the stationary like paper, files etc. But after the electronic media only require the computer and printer. This is very chip with respect to other stationary so cost is reduced.

**2.2.3.3 Transparency** – Development in the electronic and all the department will goes to online and maintain the electronically records and every thing online so that it became very helpful to reduced the corruption and increased the transparency of work. Transparency is maintained if the entire citizen will be able to access the information about the work and this information provided by the government departments.

**2.2.3.4 Accountability** – Transparent government also an accountable government. It gives the power to government give the answer of every question of citizen. Transparency and accountability also make the government answerable. A responsible government is also an answerable.

- E-governance give the esurience about the public welfare works, it make easy to all information and feedback of government works, also reduced the corruption
- E-governance make the transparent all the department and aware the citizen about our work, this is the revolution change in government
- All the information are available on the e-governance regarding the government departments so the citizens are able to actively involved for making the good and valuable decision
- E-governance makes all the process very simple through the accumulation of information



- E-governance makes the information available regarding the government department so the all department make responsible and encourage the department for doing our work properly and efficiently
- E-governance offer better delivery of services to citizens, improve the empowerment the business and industries interactions for better managements and cost reductions
- E-governance make the closer relationship between the citizen to government
- Enhancement of the E-governance make very easy to touch with the government organization/offices
- E-governance makes the citizen centre between the citizen and get easy to access and pay our bills, book tickets, make online fees for governments exam
- Development of e-court and e-police every citizen access current status of cases and see the record of criminals or current progress and investigation status of any cases
- E-governance always help to enlarge the business with the help for providing the current information of trading and decisions of government

## **2.3 Unique Identification Card (UID)**

### **2.3.1 Introduction**

In India, 27 January 2009 it is great day in Indian history, on this day Unique Identification Authority of India (UIDAI) was established. At the beginning of this project it is imagine covering nine different states and four union territories. So the resultant the Unique Identification number (UID) is issued firstly in Tamil Nadu, West Bengal, Andhra Pradesh, Maharashtra, Orissa, Gujarat, Karnataka, Goa and Kerala and the also issued in the union territories of Lakshadweep, Andaman & Nicobar Islands, Dadar & Nagar Haveli an Puducherry. At all these placed the Unique Identification card (UID) shell be issued firstly and the target to completely in 2010 early. UIDAI is expected to provide UID to around 60 crores people in 4 to 5 years [29].

### **2.3.2 What is UID (Unique Identification)?**

The ways in which such a system is applied is dependent on the country, but in the majority cases, a citizen is allocate a number at birth or when they get in touch legal

age (normally the age of 18). Noncitizens are allocating such numbers when they come into the country.

UID number is 11 digit numbers that are show the unique id of every Indian citizen. UID number should be describes as following:

1. (S1-S3) 3 digit represent to state (000-999)
2. Digit (4 & 5) for serried allocated to district by state (00-99)
3. Digit (6 & 10) is a serial number (00001-99999)
4. 11<sup>th</sup> digit use for checksum

Algorithms used in UID is (modulus 10)



Figure 2.6: Aadhaar Card on India

### **2.3.3 Legal amendments made to facilitate the project**

The Citizenship Act, 1955, has been amended and now a specific section on registration of citizens & issuing cards has been included. In addition the Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003 has been notified. (This is clearly defined all the law in the Annexure - I)

## **2.4 Other Countries**

### **2.4.1. United States**

The US Federal Government has taken several initiatives that encourage and enable citizen engagement. Since 2009, the US government has launched a 3-phased online citizen engagement project, which includes brainstorming for new ideas, seeking ranking of ideas received and incorporating them in policy making. A web based platform has been created and hosted at Challenge.gov that encourages people from all walks of life to contribute to highly technical issues such as space exploration to every day challenges related to public services (<http://challenge.gov/>). In Dec 2010, the US government sought public feedback on a concept for next generation citizen consultation, namely a government-wide software tool and process to elicit expert public participation "ExpertNet" [30].

### **2.4.2. Canada**

The province of Ontario in Canada has a long history of active citizen engagement. Since the early 2000, the state government has been seeking inputs from public and public servants into policy making. In 2003, the government launched the OPS Ideas Campaign on improving public service delivery. Later in 2004 an active campaign to engage public for improving municipal services was launched [31]. The Canadian Index of Wellbeing (CIW) is considered the world's leading example of a national system of comprehensive, citizen-based progress and well-being measures. It began in 1999 with a national consultation of Canadian citizens to identify core national values and key aspects of well-being. The Index built a collaboration of representatives of community, universities, business and some government agencies, including the national statistics office of Canada. A framework of eight dimensions forms a framework for measuring the state of national engagement; community vitality, democratic engagement, education, environment, healthy population, leisure and culture, living standards and time use. The Index has begun to generate comprehensive reports on the state of democratic

engagement in Canada and forms the basis for discussion of key aspects of citizen engagement and the models available for increasing these [32].

#### **2.4.3. United Kingdom**

The UK Government had released a citizen engagement framework in 2008 that sought to deepen engagement with public on a wide variety of issues including constitutional change, policy formulation, behavioural issues e.g. smoking etc. [33]. These efforts were further expanded through a Digital Engagement Blog [34]. The website classifies data based on domains e.g. health, local government etc., provides applications or Apps for mobile devices and provides datasets. It also provides platform for blogs, wiki, resources etc. [35].

#### **2.4.4. Brazil**

The city government of Porto Alegre practices “participatory budgeting”. This practice convenes neighbourhood, regional and city wide assemblies in which participants identify spending priorities with around 50,000 residents regularly participate. Since the practice was established a range of improvements in governance, well being and citizen engagements have been achieved, with almost tripling of an increase from 75 to 99% of homes having running water and the number of public schools [36].

#### **2.4.5. Australia**

The Australian government has planned a new vision has been completed in 2020 with name of Queensland called Toward Q2. In it completed approximately five wishes (Green, Strong, Healthy, Smart and Fair) that pointed the future and current challenges. Toward Q2 is also be directly supported by the MyQ2. For the citizen engagement this government used to MyQ2 program in which assemble all the requirements of the governments. In addition to the traditional form of participation in policy development, the government has established a wide range of unique mechanisms and tools at the state and local levels, empowering citizens and communities to be more directly involved in government policies and processes [37].

**LITERATURE REVIEW**

---

**3.1 Introduction**

E-governance is the major and essential part of the E-government (Digital Government), here the little question rise that “What is the E-government or Digital Government?”, the answer is that – E-governance make the easy governments operations and describes the technologies uses in briefly. It is directly interact with the electronically and non-electronically applications in the government. It also enlarges and improves the electronic use in government departments. It enables to all the departments to use the fax machine, record tracking and surveillance system with the help of RFID, even also made the online surveillance in examination and all the sensitive areas like railway stations, bus stand and airports. Through the E-governance information provided to all the citizens regarding or related to government.

E-government means the ‘Electronic government’ refers to ‘The ultimate use and enhancement of the efficiency in service delivery through the use of Information Technology (IT), Information and Communication Technologies (ICT) and all other web/internet related telecommunications technologies in the public/citizens areas’[38].

Strategies of digital government or e-governance is defined as ‘All the information and services are available for the citizen through the help of internet and world-wide-web regarding to the governments’[10].

**3.1.1. Literature**

E-governance is very immerging concept in recently, but there is no any proper definition every organization or company or government and person use this or define in own words or as per our intension they will modified the previous definition. Actually the E-governance is a part of E-government. We discuss some popular and widely used definitions that are listed below here:

Information and Communication Technology (ICT) used by Electronic governance in different stage of public and government sector. Main purpose of using ICT at different is increasing the governance system [45].

*“For all formal & informal activities of institutes are involved in governance, for the guidance and control the current activity. Formal responsibility created by the government, it also beehive like an authority. It is not required to be conducted by the government or non government organizations (NGOs), private or associated firms. It is*

*only required to association with governmental bodies for governance creation and sometimes it is created without government authority.”*

For this definition we all are clear in our mind that only public sector is not limit of e-governance. It is also implemented in the private sector with all the administration policies and managing strategies.

According to the UNESCO e-governance is: *“E-governance is using the information and communication technology for the public sector’s the main objective is enhance our services with better information delivery and for better decision should require the involvement of citizens with better transparent, effective and accountable government. E-governance give the batter opportunity for implementing new style of information delivery, new style of services, new style of listening citizens complaints, new style of debate and policy making, new style of investment, new style of education and new style of leadership. In government, e-governance is a wider concept of citizen to government or vice-versa. In all this type of relationship required the responsibilities and citizen needs. Its aim is to give the power to citizen and grow of citizen.”*[39]

According to S. Clift, it is: *“Actually E-governance build by E-democracy. Its main aim is to enable development and innovation under the Information and Communication Technology (ICTs) and also included motivation of high level democracy and targets.”*[40]

According to Council of Europe, E-governance is an electronic technology and it is also divided into three different public areas of action; make a relationship between the citizens to government society; work for all stages of the government authorities by the process that is called the electronic democracy; availability of services for citizens (electronic citizen service) [41].

In another words according to the Council of Europe, it is: *“Electronic governance application means: 1) Increase communication between citizen to government and businesses to government; 2) for improve democracy simplify the domestic operations and business aspects from government to governance”* [42].

According to D.F.kettl e-governance is; *“It is a method to express the interaction between the administrative, political and social (broader environment) to government”* [43].

UNESCO also give the another definition of e-governance is: *“Governance is used the country’s affaris, authority of administrative, political and economic and also taking the obligations and legal rights of citizen. E-governance helps to understand the government transparent, efficient and speedy process via the electronic medium and easily*

*spread information between agencies and public organization and doing administration activities perfectly” [39].*

According to AOEMA report of World Bank, E-governance is: *“E-governance refers information technology is also used in government agencies just like work in mobile network, Wide Area Networks and the internet for the relations transform between the government to citizen. It works just like the right arm and left arm of the government. These emerging technology also serve different variety of services like: enhance the government service delivery to citizen, enhance communication between the industry and business, give the right to citizen for access the information directly and better way of government management. The resultant enlarge transparency, decreased the level of corruption, improve conversation and convenience, decreasing the cost and also enlargement of revenue generation” [44].*

According to the S.K.Sharma, E-governance is: *“For the central, local and state government, E-governance is web-based standard application. Using information technologies in e-governance enlarge the government operations, provide better services and also connect all citizen to government. Using the e-governance citizens empower for make fearless online payment, taking information about the work, aware about our right all these things are done by the using of World Wide Web” [45-47].*

According to United Nations, e-governance is: *“For delivery the information of government and other services to citizens this is the best way as compare to World Wide Web and Internet” [48].*

In AOENA report according to Global Business Dialogue on Electronic Commerce (GBDe), e-governance is: *“For the public service provision all the state and central judicial, administrative and legislative agencies are utilize internet for all internal and external operations are become digitize and citizen unitize the better services from the government agency’s sides” [49].*

According to the Gartner Group’s it is: *“Using the Internet and Communication governance deliver the optimized service, contribution of the external and internal constituency relation through this technology” [50].*

Another definition given by Gartner it is; *“Involvement of Information and Communication Technology (ICT) in e-governance, enhance the government services and operations for the citizens and make the emergent and transparent nation” [50].*

According to the E-governments Working Group it is: *“Information and Communication Technology (ICT) using in e-governance for encourage government to give more assists and easy accessible services and governments information and make accountable government. In which also include wireless devices (i.e. telephone and mobile) and wired/wireless Internet for providing more facility from government to citizens. These services are either self or facilitate by others like call centres”* [51].

According to all of them but there is one common theme is: *“For involvement of Information Technology in e-governance improve the government service delivery to citizen and other government or private agencies specially with the help of internet. E-governance empowers citizen for the accessing the central, state and local government services and information for 24by7 days. It is the early stage of development of government. Most of government are worked in it and remaining is going to start this facility. Nevertheless the actual power of e-governance is reconstructs the government and transforms long business processes”* [52].

According to C.Leitner it is: *“It is functionally change in nation government and develop new processes for the public services that are delivering and generate by the government and also changing in the complete range of citizen to government, government to business relationship.”* [53].

In presently the growth in wireless communication e-governance is now coming in it. Now the e-governance is change into the m-governance. M-governance meaning is ‘Mobile Governance’ means that all the facility and services are also available at the citizen’s mobile/cellular phones, Personal Digital Assistants (PDAs) and on laptop, tablets. After completing the m-governance implementation this is the replacement and more empower rather than e-governance.

So the after reading and discussing all this valuable definitions we know that after using the information & communication technology (ICT) the e-governance delivering more efficient services and interact of government to citizen is improve also reducing the cost in every process is done in the government offices so the resultant the more revenue is generated and after the successful implementation the government will going to be more transparent with respect to present.

## **3.2 E-governance of India**

### **3.2.1 Information Security Assurance Framework**

#### **3.2.1.1 Information Security**



E-Governance involves Information Technology enabled initiatives that are used for improving the interaction between Government and citizens or Government and business as well as the internal Government operations. To provide “trusted” services, e-Governance needs to focus on Effectiveness, Efficiency, Flexibility & Transparency [54].

If the citizen or end user is to derive maximum benefit from the provision of e-Services through e-Governance, the e-Service must possess the following attributes.

- The users must know the information about the available e-services;
- The users must be aware of the benefits of these services;
- The user should be able to locate the e-services easily;
- The e-services must be accessible to all members of the intended target groups;
- The information from the e-services should be comprehensive, correct, readily available, and easy to understand with respect to language and structure;
- The provision of e-services should be confidential, and in no way violate the privacy of either party;
- The design of e-Governance applications should comply with the existing legal data protection requirements and relevant legal and statutory laws & acts.

From the attributes it becomes evident that the “value” of information held and processed by the e-Governance service needs to be protected at all levels (i.e. Application, Infrastructure, and Operation & Management) [54]. Information security is intended to safeguard the information assets and is determined in terms of confidentiality, integrity and availability.

**Confidentiality:** Protecting sensitive information from unauthorized disclosure or intelligible interception

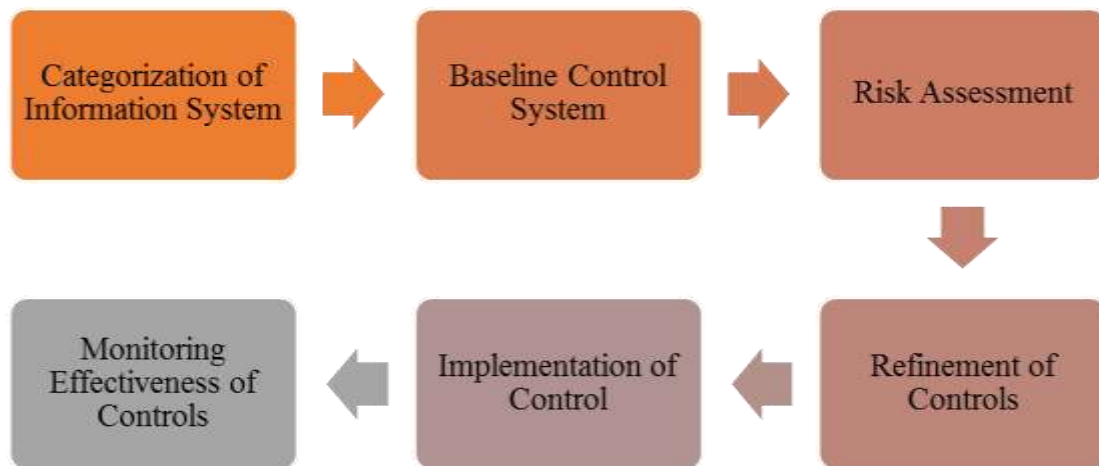
**Integrity:** Safeguarding the accuracy and completeness of information and software; protecting data from unauthorized, unanticipated or unintentional modification

**Availability:** Ensuring that information and vital IT services are available when required

To safeguard the “value” of information, effective security measures (that can limit the risks and vulnerability) need to be implemented harmoniously. These security measures provide layers of protection to the Application, IT Infrastructure and Control & Management in an e-Governance computing environment.

In fact security of any information system is essentially an amalgamated output of Application Security, Infrastructure Security, and Secure Operation & Management.

Enforcement of security at all levels is essential to achieve a fairly secure environment [54]. As the probability of simultaneous failures of security at all layers is less this approach has been found to be the most effective in to-day's context. This layered approach is alternatively known as 'Defense in depth'.



**Figure 3.1: Current E-governance Assurance Framework**

The key activities in assuring information security are

**3.2.1.1.1 Categorization of Information System** – The security classification are completed on the basis of possible impact on an company, should various incidents produced which is needed the information system for an organization to achieve the allocated task or project, they also meet all legal responsibilities, organized its day-by-day tasks and secure being. Security categorization should also consider the vulnerability and threat information corresponding to the information system [54]. All information systems can be categorized as Low Impact, Medium Impact and High Impact depending on the assessed impacts. A document (GD 100) provides guidance for this purpose.

**3.2.1.1.2 Selection of Baseline Security Controls** - Baseline Security Controls are the minimum information security requirements (Application Security, Infrastructure Security and Operations and Management Security) for information and information systems in each security category (Low Impact, Medium Impact and High Impact). A guideline document (GD 200) provides a list of all possible security controls and serves as a master catalog of all security controls. Baseline security controls are subset of controls taken from the master catalog. There are three baseline documents Low Baseline (GD 201), Medium Baseline (GD 202), High Baseline (GD 203) [54].

- *Low Baseline*: Subset of basic level security controls taken from the master

catalog of controls.

- *Medium Baseline*: Builds on low baseline with additional controls taken from the master catalog of controls.
- *High Baseline*: Builds on medium baseline with additional controls taken from the master catalog of controls.

**3.2.1.1.3 Risk Assessment** - Over and above the baseline security controls depending on the operating environment and technology there can be some specific security requirements. These security requirements can be identified through a risk assessment process. Guideline document GD 300 outlines the risk assessment and management methodologies.

**3.2.1.1.4 Refinement of the Security Controls based on Risk Assessment** - Based on the outcome of the risk assessment additional controls or control improvements may be selected from the master catalog of controls.

**3.2.1.1.5 Implementation of the Security Controls** - After identification of the security controls it is necessary to implement the security controls in the respective information systems through managed processes. A guideline document GD 210 outlines implementation guidelines in details [54].

**3.2.1.1.6 Monitoring and Analysis of the Effectiveness of the Security Controls** - Monitoring and analysis of the effectiveness of the security controls can be conducted through periodic testing, evaluation, review of the implemented controls. A guideline document GD220 outlines the procedures of assessment of the effectiveness of the implemented security controls.

### **3.2.2. Policy of E-governance in India is clearly defined in the Annexure - II**

## **3.3. Unique Identification Card (UID)**

### **3.3.1. Legal Framework**

The Constitution of India, through the Directive Principles of State POLICY mandates that the state shall strive to minimize inequalities of income and end eavor to eliminate inequalities in status amongst individuals. The objective of the UIDAI is to solve the key problem of identity that individuals face and enable better and efficient delivery of services to the poor and marginalized so as to eliminate inequalities of income and status. It is therefore, imperative to have a proper legal structure in place to ensure the smooth functioning of the UIDAI [55]. This section provides an overview of the legal and policy framework.

For the setup of Parliament Act the Unique Identification Authority of India (UIDAI) has been work as a legal body. The UIDAI will be authorized:

- To collect the following identity information from any person voluntarily seeking a unique identity number:
  - ❖ Name
  - ❖ Date of Birth
  - ❖ Gender
  - ❖ Father's name and UID number
  - ❖ Mother's name and UID number
  - ❖ Address
  - ❖ All ten finger prints, photograph and both iris scans.

Collecting the information and information permission against make a law, this is say that stickle not permitted regarding the religion, cast, ethnicity and other similar information collection publically, and not give any facilitation analysis the information regarding the citizens for profiling and similar activity.

- To issue a unique identity number to the person who has provided the necessary information and fulfilled the requirements as laid down in rules prescribed by the UIDAI. To verify the identity of any person at the time of the provision of information, the issuance of a unique identity number or at any other time per the UIDAI database or other possible means, as laid down in rules prescribed by the UIDAI [55].
- To permit the UIDAI to set up or facilitate the infrastructure by which third parties can authenticate the identity of persons who have provided information to the UIDAI and the circumstances and conditions they can seek such verification. Authentication identification is only done with the help of stored database information.
- To establish or appoint a Central ID Data Repository (CIDR) for the purposes of collecting, managing and securing the database and to outsource any such functions.
- To permit the appointment of Registrars in accordance with criteria laid down by the UIDAI to enrol people that seek unique identity numbers directly or indirectly through enrolling agencies [55].
- To allow for the appointment of other service providers in accordance with criteria laid down by the UIDAI, as the UIDAI may deem fit to further its objectives and to ensure efficiency.

- In these a new service provision for the record and information is that produced any type of audit, inspections and inquires against for the enrolling agencies, registrars, service provider and CIDR.
- To enter into all necessary contracts and arrangements in order to fulfill the objectives of the UIDAI.
- To setup mechanisms for grievance redressal for the public
- To setup a monitoring framework to improve implementation, create safeguards as required and study the impact of the UID
- To hire the necessary technical and professional personnel necessary for executing the mandate and fulfill the objectives of the UIDAI [55].

The law will contain many acts this is clearly defined in the Annexure - I

### **3.3.1.1. Protecting Privacy and Confidentiality**

General information is also available in many government or private agencies/organizations database but only the biometrical information (i.e. IRIS & Fingerprint record) is stored in UIDAI database. Unique Identification Authority of India (UIDAI) is stored the very private and personal data of citizen so these protection is so much required to secure and also in the central database the idea's given by the citizen is stored in it. Here the privacy of all the citizens data is required with use of high level of mechanism. Unique Identification Authority of India (UIDAI) is stored the privacy of the citizen seeking with the help of unique identification number of his/her. This type of information is only used for the identity authorization with the matching with stored information in the database. Here the necessary conditions are to maintain the confidentiality and privacy of stored information in the database [55].

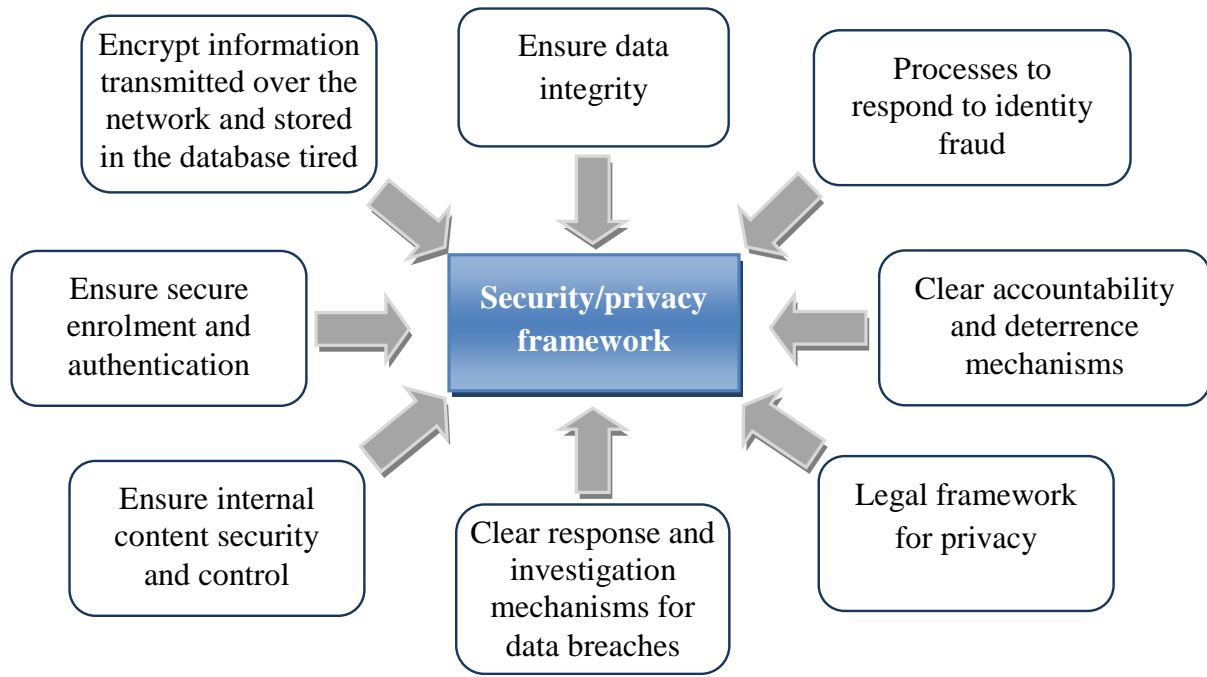
### **3.3.1.2. Data Security and Fraud**

#### **3.3.1.2.1. Protecting Personal Information of Residents**

Even as the UIDAI stores identity with the resident information and confirms for authentication, this is give the surety for all the information is make confidential and secure and not used against the citizens. Through the UIDAI, it makes the easy to transfer the resources and money with use of reliable and verified, and personal information and identifying information linked with the UID to UIDAI [29].

This is not only stored the biometric information but also the private and personal information regarding the citizen. For protecting the information, the information is classified means the personal information like address and non-sensitive data is not linked with bank transaction or financial information. Only the identity information is linked or attached with the passport service, banking transaction and social security, identity information like biometric records (i.e. IRIS record or Fingerprint records). For the credit

card, online bank accounts will require or verified by the data of birth (DOB) of citizen. All this information has to be secured. In the case of identity theft or misuse of personal information of citizen, the information is loss or licked by the any person or hacked by the attacker, this is very serious situation and increased the risk for loss the financial information regarding the citizen. In the federated system that the UIDAI envisions, we must consequently have processes in place to ensure a fair level of data security [29].



**Figure 3.2: Security/Privacy framework for Unique Identification Card (UID)**

### 3.3.1.3. Technology architecture of the UIDAI

The technical architecture of the UIDAI is at this point, based on high-level assumptions. In the UIDAI architecture whiles a very high level of information security and privacy of data is maintained. This is structured architecture to give empower of high level information security and well structured authentication, verification of data and stopped the duplication of data.

#### 3.3.1.3.1. System architecture

The central database gives the central ID for data repository to all the citizens, it contain the confirm identity with the limited fields of information. Information regarding to citizen all are stored in the registrars and after that merged in the central database, and accessing this information make the key, it's called the UID [55].

For the UID system the key technology components are:

##### 3.1.3.1.1. The UID Server, this is provided the authentication and enrolment facility.

This facility makes the registrars and their authentication services to online use. The server backend required the high demanding architected that is work on the concept of

1:N for stopping the duplication of biometric authentication as well as the other authentication services [31].

**3.1.3.1.2. The Biometric sub-system,** this is the heart of the UID system, gives empower for authenticate or enrolling the citizen with in the system. For get the high level of assurance will be required the multi-modal biometric solution. This is used the multiple-biometric modes for get the employed acceptably performance and also used distributed processing, hashing, in-memory database and indexing in database and 1:N concept for the UID system used the computing-intensive operations [29].

**3.1.3.1.3. The Enrolment client,** this is required the biometric and demographic data for validate and capture the application. The village's people required to work offline mode because there the no internet connections and they required upload a batch file for processing into the server. If the uploading is not possible the file is transporting physically for the uploading at the CIDR office. On the standard workstation for enrolment required to deploy the client application [33].

**3.1.3.1.4. The Network,** give the power to authenticate and enrol new UID's online. This is a very significant characteristic of the system. The UID should not only used the vanilla internet, mobile SMS channels for secure WAN networks but also works on the Point of service (POS) that is used in credit card devices [8].

**3.1.3.1.5. The Security design,** in the UID system for physical or logical attack required the several components like:

- **Server Security** – intrusion Prevention and Detection System (IPS & IDS), Firewalls etc.
- **Network, Client Security** – Public Key Infrastructure (PKI), Crypto analysis, Encryption & Decryption, Network analyzer Tools etc.

The administrator providing help to UIDAI's process with the regarding of administration this include:

- Account setup – for the agency, new registration, enrolling for authentication or make the modification in the exiting account [56]
- Role based access control – Over the UID resources, allocate several rights on the role based
- Audit trailing – for the UID system follow all the right of entry [56]
- Fraud Detection – Using the audit trails easily identified the identity theft or any other cyber crime is done
- Reporting an Analytics – for making the report and analysis the system using Visual decision support tools – GIS, Charting etc [56].

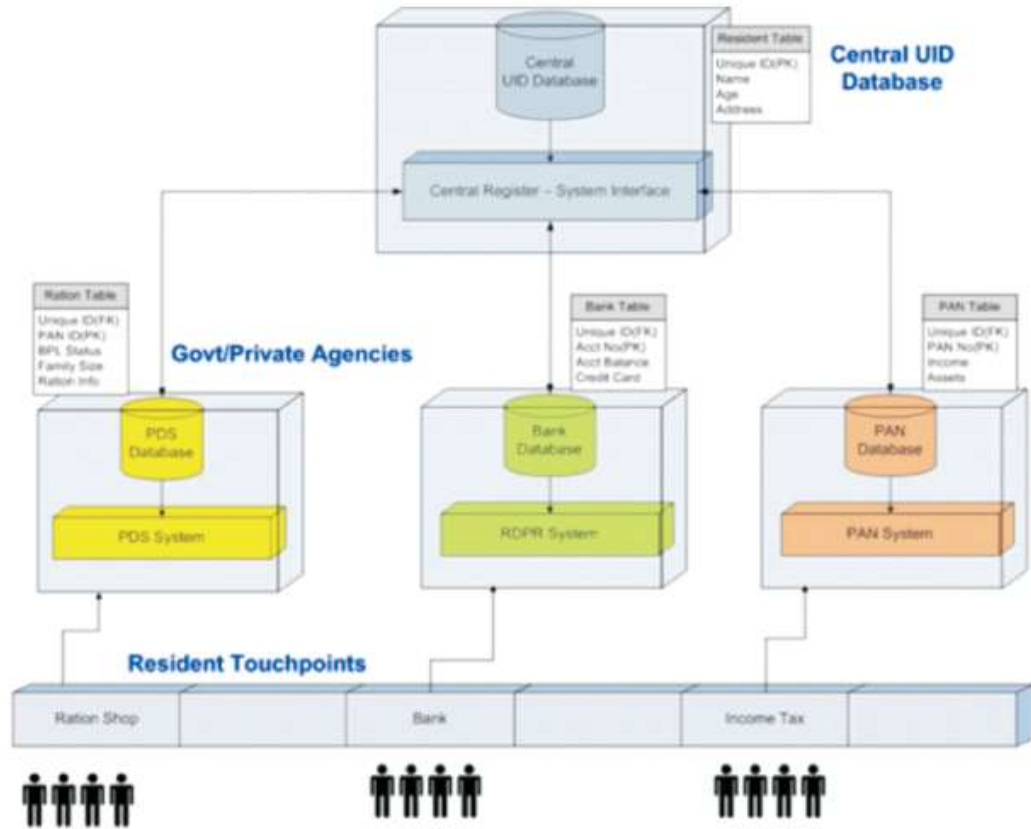


Figure 3.3: Central UID Database system architecture

### 3.3.2. Aadhaar Authentication and Current Framework

Aadhaar Authentication is the process wherein, personal identity data along with Aadhaar number is to be submitted in the Central Identities Data Repository (CIDR), also matching with the Aadhaar holder's identity information on the basis of CIDR available information with it.

Authentication shall enable residents to prove their identity based on the demographic and/ or biometric information captured during enrolment, thus making the process of identification convenient and accurate. Aadhaar Authentication shall make life simpler for residents and eliminate the distress and inconvenience in establishing their identity for availing services [56]. Through Aadhaar Authentication, more residents shall be able to prove their identity and thereby become eligible to benefit from Government schemes and subsidies. Aadhaar Authentication shall help AUAs in delivering services to eligible beneficiaries based on establishing their identity, thus improving efficiency and transparency in service delivery to the common man [29].

Aadhaar is a permanent and non-revocable identity as opposed to currently existing identity systems which are based on local, revocable credentials. Hence, AUAs are encouraged to use Aadhaar Authentication in conjunction with the AUA's existing



authentication process so as to strengthen their authentication process. Aadhaar Authentication should be perceived as a mechanism to strengthen the current authentication process followed by AUAs to authenticate residents/ beneficiaries and enhance the level of identity authentication assurance while providing convenience to the resident [55].

It should be understood that the Aadhaar authentication system is not a 100 percent accurate system, irrespective of the kind of attributes selected for authentication. In cases where Authentication Device operator has sufficient reason to conclude that the outcome of an Aadhaar authentication result is not accurate, the operator may explore alternate mechanisms, including verification of Proof of Identity/ Proof of Address documents for establishing the identity of a genuine resident. The AUA shall put in place practices and procedures for handling exceptions so as to deliver services to all genuine beneficiaries.

Aadhaar Authentication supports:

1. Demographic Matching
2. Biometric Matching and
3. Additional features such as One-Time-Password (OTP)

#### **3.3.2.1. Demographic Matching**

Demographic matching refers to the usage of Aadhaar Authentication system by AUAs for matching Aadhaar number and the demographic attributes (name, address, date of birth, gender, etc. as per API specifications) of a resident in the CIDR with the data in the AUA's database or with demographic data submitted at the point of authentication [29].

For example, demographic matching could be used by:

- Banks for automated KYC checking
- Any government welfare scheme for eliminating fake and duplicate identities in their databases
- Telecom service providers for address verification
- Private institutions/ banks for date of birth verification

#### **3.3.2.2. Biometric Matching**

Biometric Matching refers to the usage of Aadhaar Authentication for matching the biometric attributes of a resident in the CIDR to the biometric data submitted by the resident on an authentication device.

For example, biometric matching could be used by:

- Banks for establishing identity of customers before starting a new bank account
- Telecom service providers before issuing a new mobile connection
- Any organization for attendance tracking

### 3.3.2.3. Matching using any other factors such as One-Time-Password (OTP)

In this case, an OTP is sent to the registered mobile phone number of the resident seeking Aadhaar Authentication. The OTP shall have a limited validity. The resident shall provide this OTP during authentication and the same shall be matched with the OTP at the CIDR [18, 29].

For example: OTP based authentication could be used by

- Banks for authenticating customers during internet banking transaction
- E-commerce companies before completing a cash-on-delivery transaction

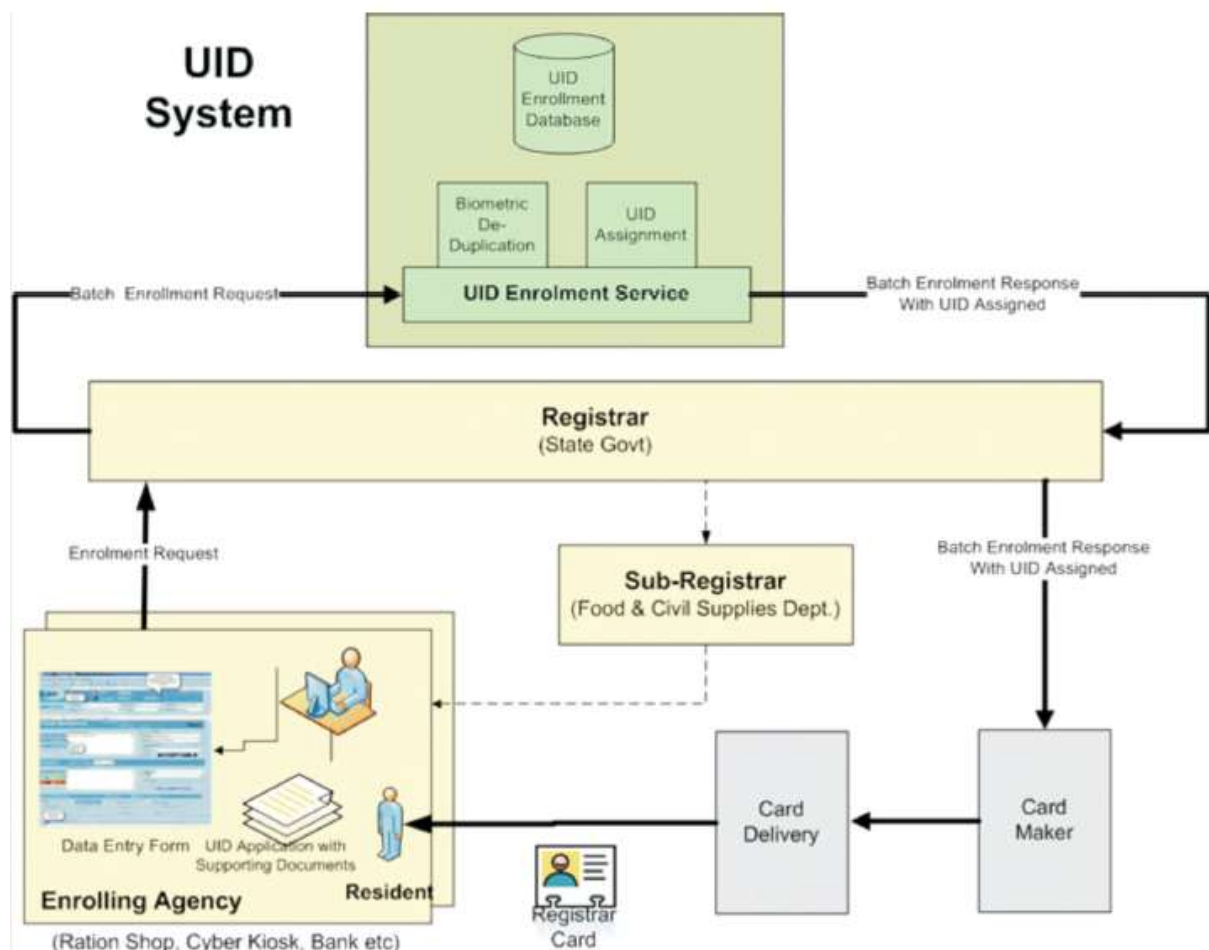


Figure 3.4: Aadhaar Authentication and Registration System

### 3.3.2.4. Issuing the UID number

UIDAI give the latter to resident in which his/her biometric and demographic details are stored after the UID number is assigned. In these latter also has the name of

person, photograph, 2D barcode which is stored the fingerprint minutiae digest along with the UID number. If card holder's found any such type of mistake like wrong name or spell of name is wrong or photograph is wrong attach then they directly contact to the Registrar or the enrolling agency for correct the information with pre-defined or recommended course of action. After allotted the UID card along with the name, photograph and UID number they will be free to attach more information to several services such as customer ID by bank or government organization [29, 55]. The UID card will become interoperable if the registrars will be stored biometric information on a single card, it is also free for storing or printing the card holder's biometric information this is stored on the card. For the offline purpose the interoperable is used. For enforce or audit the UIDAI would not be insisting. On the behalf of registrar all the data collection is done only in English language from the authorized agencies [29].

If the registrar want to verified all the information in local language they have right to convert the information with the help of standard transliteration software. The UID number latter sends by the UIDAI that is contain all the information with the local language of the citizen's belonging state and also with the English language [56]. Election Commission of India gives this instruction of allocates the UID with both local & English language so that this is followed by UIDAI.

UID Registrar	Primary Access <sup>1</sup>	Additional Acces <sup>2</sup>	Potential Overlap	Effective Enrolment
	Crore Residents			
LPG (Oil PSU)	8.4 <sup>3</sup>	16.8 <sup>4</sup>	20%	20.2
LIC (Life Insurance)	13.5	13.5	50%	13.5
PAN Cards	4.0	-	75%	1.0
Passports	6.0	-	80%	1.2
Urban Enrolment				35.9
Lic (Life Insurance)	3.5	3.5	90%	0.7
NREGA	10.0	20.0	10%	27.0
BPL Ration Cards	7.0	21.0	60%	11.2
State BPL/APL	15.0	45.0	50%	30.0
Old Age Pensioners	1.5	1.0	70%	0.8
Women/Child Welfare	1.0	2.0	70%	0.9
Social Welfare	1.0	2.0	70%	0.9
RSBY	0.5	1.0	70%	0.5
Rural Enrolment				72.0
Total Enrolment				107.9

**Table 3.1: Stage of various services that is using UID**

#### 3.3.2.4.1. Type of Authentication

UID authority should be offered to multiple authentication forms. If the card is forged there are various type of authentication shell be low to medium are available. Here we are give the short discussion for the authentication main forms that is directly or indirectly depending on the situation or available equipments [29, 55].

UID system shell be support to **Online authentication** in this can be attached

- At the medium assurance level, the authenticating agency should be compare the demographic information and UID number to stored with the database information for online demographic authentication
- At the high level of assurance, biometric authentication is done for the biometrics of the UID holder, key and his/her UID with the CIDR's details are compared with demographic details.
- Level of assurance is not decided because if the biometric authentication is done then the assurance is high or if the demographic authentication is done then the assurance level is medium. For the UID system authentication, a programmatic call is generated by the registrar's system that is authenticating with APIs, along the API both biometric and demographic authentication is used [29].

UID system also supported the **Offline authentication**, its not be used by UIDAI service provider, it's only supported by the registrar. This is done in two different forms.

- The assurance level is low if the photo authentication is done. At this type of authentication the cardholder's face matched with the photo on the card
- The assurance level is medium if the scanned fingerprint is compared with the stored biometric. This is called offline biometric authentication [29].

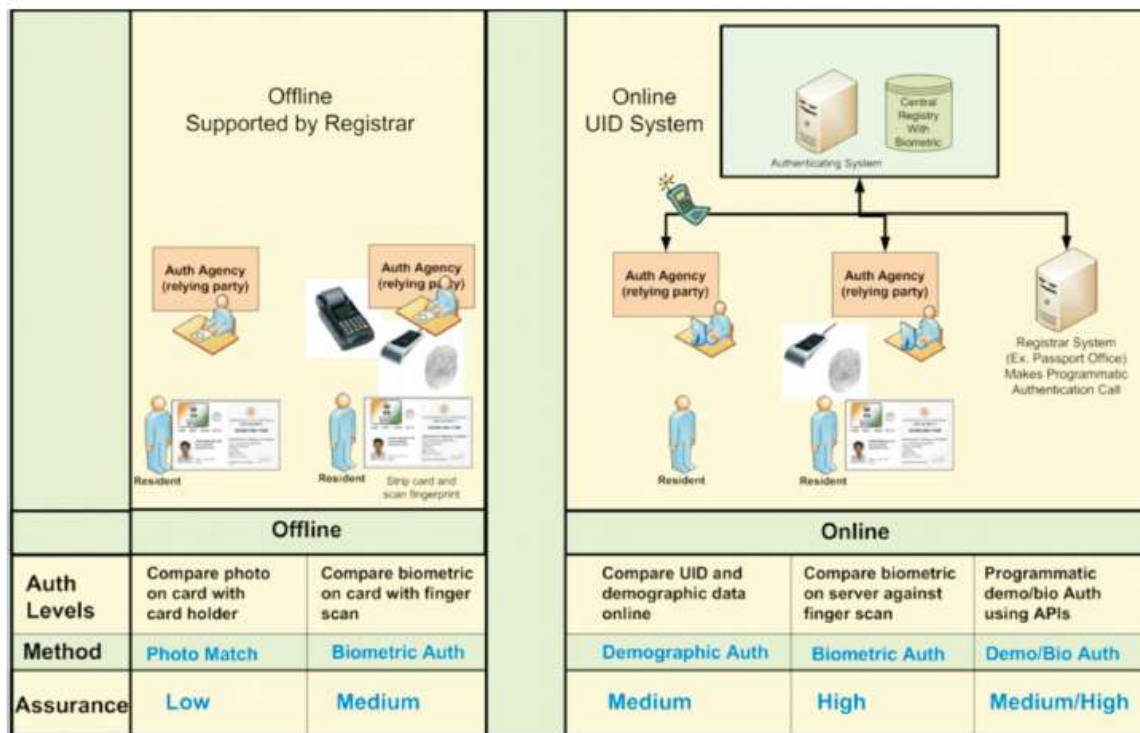


Figure 3.5: Offline/Online Registration in UID System

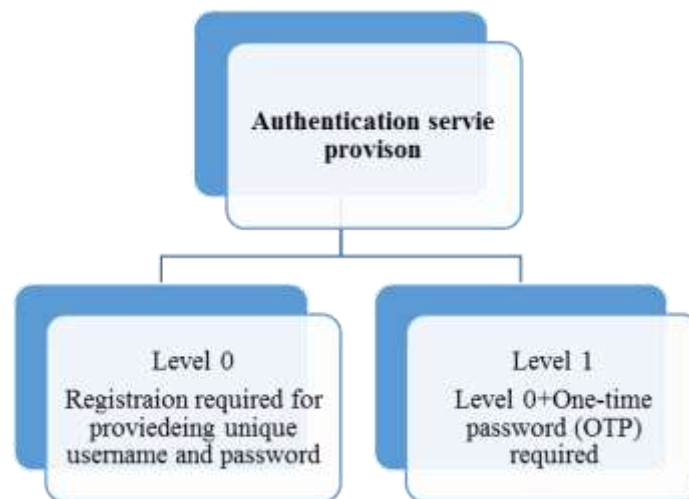
## DEVELOPMENT OF SECURITY FRAMEWORK

### 4.1 Critical Analysis of Existing Model

There is a useful discussion found throughout the literature reviews that examine the current framework of e-governance of India. Current framework has been developed either by traditional framework or by technologists focusing on encrypted data. The major limitation of existing framework is that no any physical authentication is done or no any backup and easy discovery is use in.

The existing framework does not cover all aspects of secure login or authorization; they are not general enough to describe fully the secure and backup process in a way which will assist the development of new framework techniques.

Result analysis of current framework has been reviewed here as mentioned in figure:



**Figure 4.1: Current Authentication service provision for accessing the data from e-governance web portal**

### 4.2 Critical Analysis of Security Technologies

Security technology should provided the system and information protection against attackers for the organizations. Each technology provided the help to protect system/information against hackers/attacks and also find the unusual/suspicious activities. Here we are critical analysis to various security technologies and find the best technology for our system. Presently we all are know the biometric technology is one of the best option for protect our information to the attacker. Several of security technologies are shown in figure 4.2 here it is.



**Figure 4.2: Different Security Technologys**

#### **4.2.1 Operational Technology**

Burglars actively seek ways to right to use networks and hosts. Armed with knowledge about precise errors/bugs, social engineering techniques and methods to take the information from system automatically penetration, burglars can often put on entry into systems with disturbing ease. System administrators face the problem not only how maximum valid user use the system services but also minimize the number of unauthorized users and complexity of network and protect the network form attacker. Data resources and assessed should be defended and unauthorized user's activities should be detected and assessed and suitable reply can be made when the security episode as they develop or occur.

#### **4.2.2 One-Time Passwords**

One-Time passwords is the another solution of authenticate a user. In one time password is time based password, just like for 5 to 15 mints as dependent of the authentication level. One time password will give them another power of user to valid his/her self or monitoring our login. For example that Gmail providing the 2-step verification process in which when the user will logon at any system the server will send the OTP on his/her mobile phone, that is entered in his/her account, that OTP is only valid for 5 mint, after that they expired automatically.

If administrator is want to improve the more security in OTP they encrypted when they traverse in the network so that the attacker will not identify them. If they capture OTP using the packet sniffers during the traverse networks not to read them.

#### **4.2.3 Cryptography**

Cryptography is another best method in security. They give the power to hidden the information during the network traverse or stored. In which many methods has to purpose like 16-bit, 32-bit, 128-bit, 256-bit encryption or many algorithms like DES, AES, Message Digest, RSA, Quantum encryption etc. In these methods the original message (called plain text) is converted in non-readable form. For example that if plain text is 100 bit long and want to send this information to another person through network then we will add the extra bit in the plain text like 28-bit if we are using the 128-bit encryption method using the public/private key according to the algorithm after that is message is converted into non-readable (called cipher text) from and send it into a network or stored. Information is received by receiver, they firstly decrypt the information again using the public/private key, and decryption is the just reverse process of the encryption.

All the process is done with the help of digital certificate issued by authorized company or government organization. When the user want to send the confidential information to other then, they will use our digital signature and encrypt the information. The major side effect of this process is that concept of non-repudiation.

#### **4.2.4 Firewalls**

Firewalls placed at a network gateway server which is provided the security to our private network and resources form the other networks attackers. It seems like a group of program. Firewall is also a program and hardware both. Firewall mainly works on the internet and also installed at the network. It allows workers access to the internet, it's provided the security form the outsider's user and also control the user who is used our data resources. The main purpose of firewall installation in the network is that it brooks all the requests and queries that are achieved the criteria of security that is established by the organization's network administrator. If a simple firewall is installed in the network the work is that they only filtering the router mean that they only discard those packets that are coming form the unauthorized addresses or seems to connect to unauthorized ports for service. Firewall as also work like the proxy mechanisms, is that hidden all the worker in the organization from the outside network only one use is available for communicate is proxy or firewall in which all the security mechanism and thread are implemented.



#### **4.2.5 Analysis tools**

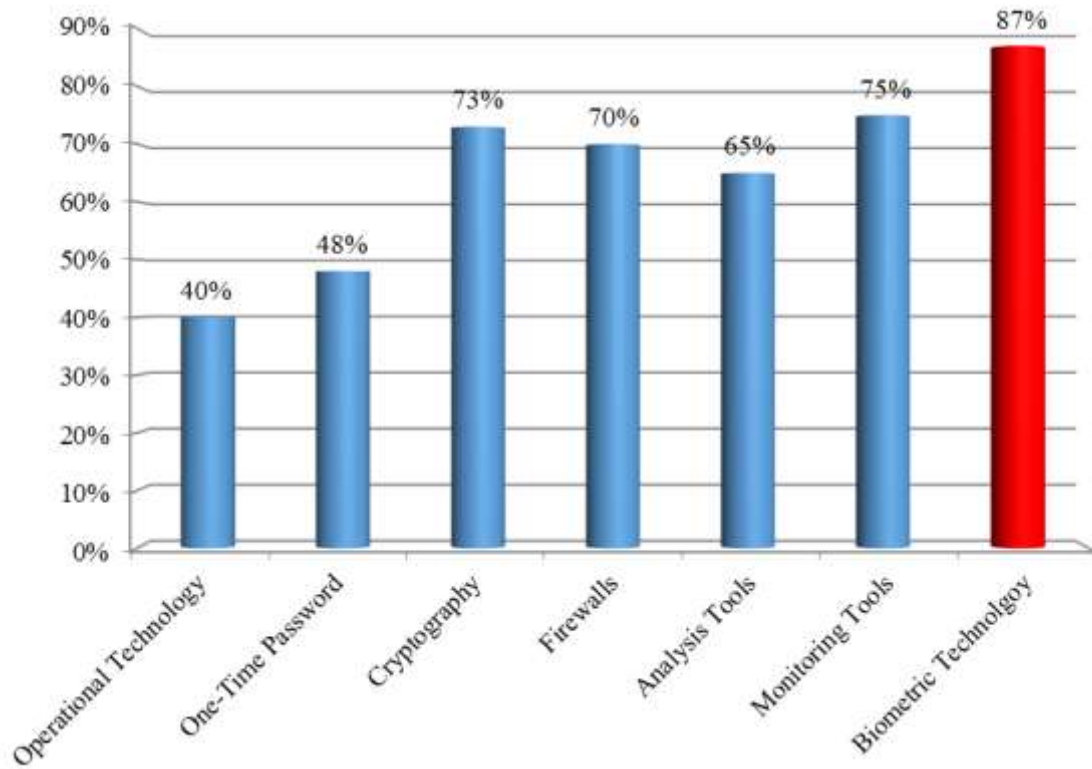
There is strong need for analysis tool because of the increasing sophistication of attacker rules and the bugs/errors/loopholes present in the used applications/system, it is very important to review periodically network loopholes to compromise. A multiple range of loopholes/bugs identification tools are present, which give the command and take the advantage to analysis the network. Analysis tools are freely available to the internet they give the advantage to analysis the network and find the threat and misused the treat for attack on the network.

#### **4.2.6 Monitoring tools**

Regular monitoring of network activity is essential if a web portal is to maintain a highly confidential data on the network. Network monitoring tools should be installed at appropriate location for collecting and regularly monitor the network and examine the data traveled in the network for any suspicious activity from the attackers. Presently it's possible in various monitoring tools providing the automatic alert system means when they found any suspicious activity in network than the issue a notification to network administrator. Most of attacker used the denial-of-service attack because the administrator is busy to solve this problem and they hack all the confidential information/data form the network or place a malicious code in the network they give regularly information to the attacker and send a copy of all the data or information automatically without knowledge to the administrator.

#### **4.2.7 Biometric technology**

Biometric technology is process of verifying or identifying an person with two different approaches is 1) physiological characteristic, in which examine the fingerprint, IRIS examine or face detection, 2) behavioral characteristic, in which check the keystroke, dynamic signature or voice verifications. They both are included in the biometric technology. Biometric technology is one of the best security mechanism for secure our private or confidential data from the attacker or various malicious activities.



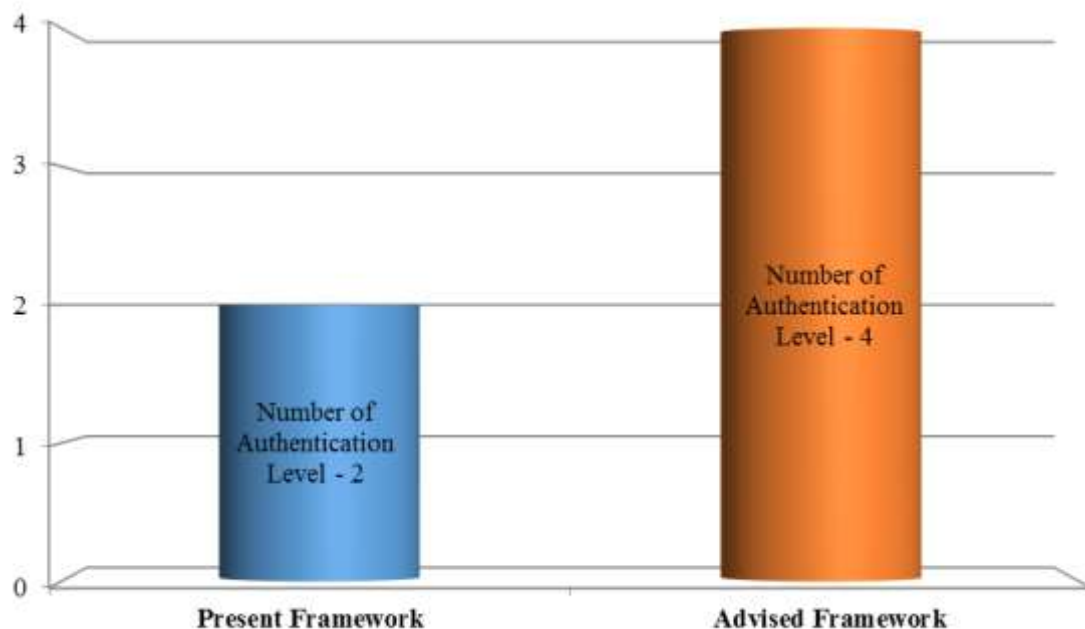
**Figure 4.3: Statically review of security technology**

### 4.3 Drawbacks of existing framework

In an E-governance plan, various and suitable amount of credentials are available to maintain the police, land, E-tendering, category/cast certificates and so on various data. Each department is critical so that only authorized person to access the network and use the data. There is need of knowledge of information security and its improvement of e-governance.

In the current running framework only two level of security is implemented. Presently no any framework is running or future in planning that the biometric authorization is used for authentication. Two level of security is very easy to break its not only loss the confidentiality and integrity of data but also loss the country's future. Its also use 46-bit SSL encryption with version 3.0 that is developed in 1996. No any plan running or is not including in future for backup of data for any disaster occurred. No any planning for easy and safe discovery of user's/government's data. Major drawback is that if any user registered it self on e-government web portal and give the wrong information there is no provision for check or verify this information.

The proposed framework attempts to improve upon existing framework through the combination of common techniques while trying to ensure method shortfalls are addressed. The proposed framework is applicable to all current digital governance, as well as any unrealized government project of the future.



**Figure 4.4: Statistical Analysis showing the current to proposed framework in respect of number of authentication level**

#### **4.4 Development of High Level Security System for e-governance of India**

A new model for security of e-governance has been described here. The inclusion of information flow, as well as the security implementation, makes it more complete than other models. The proposed model has various phases as: Registration & Authentication framework, E-governance services framework and Backup and e-Discovery framework.

Each phase has its own importance in the model and is placed in sequence. The sequence goes like this: Registration & Authentication framework is the mirror of communication of individual user in the system, in which level of authentication should be improved at different levels to complete the identity of user. E-governance services have organized the different services of government like how user data should be secured and confidential in database; how user's information should flow in the government system. Backup and e-Discovery describe how user would navigate the data intelligently in the database and if any disaster occurs, then how data is saved and restored in system properly.

**Figure: Purposed framework for e-Governance security enhancement**

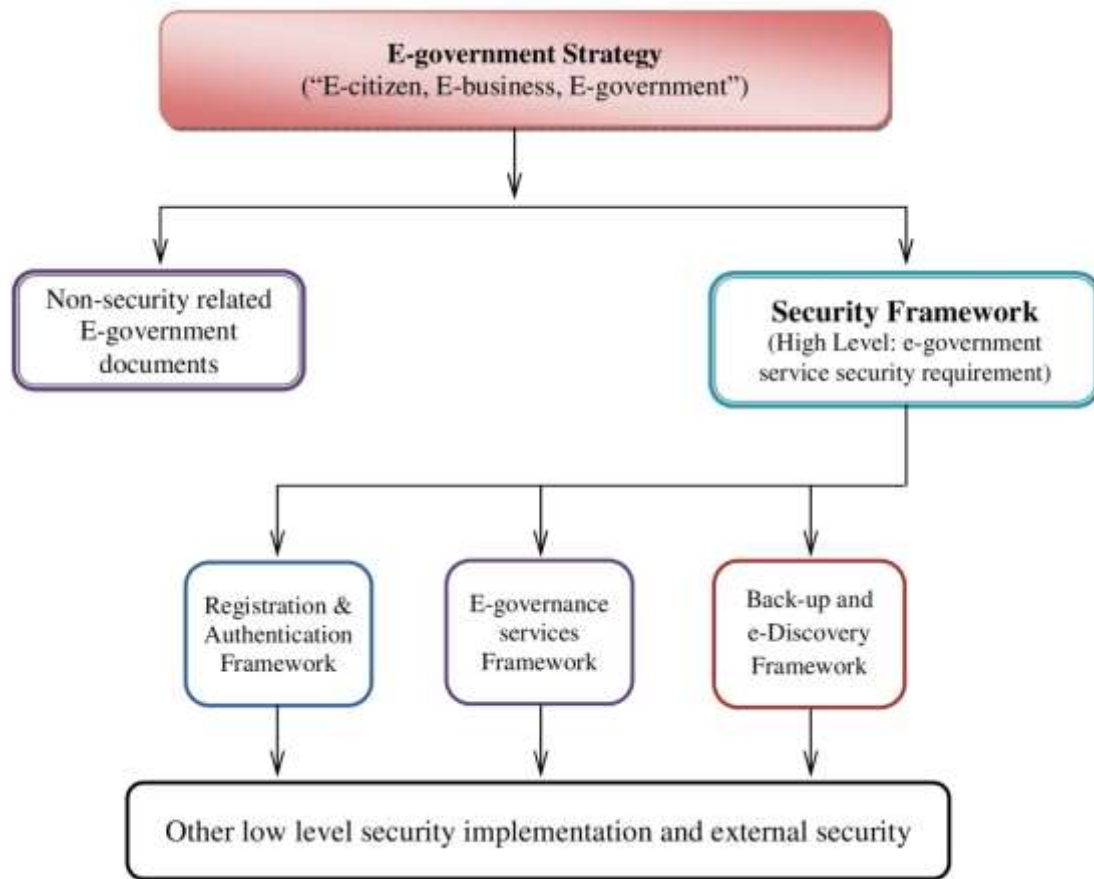


Figure 4.5: Purposed framework for e-Governance security enhancement

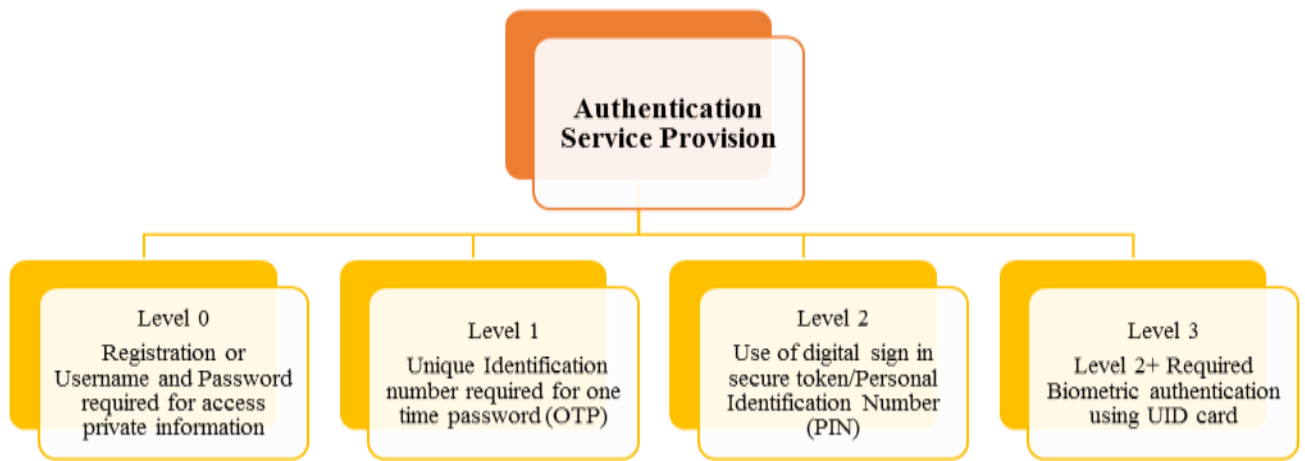
#### 4.4.1. Registration and Authentication

Registration is the process for access restricted services/document. Registration and authentication process is both are implemented parallel at the same time. Actually the major differences between the both the process is that the registration process the user is give the personal information like name & password for login, E-mail id, address, mobile no etc. But in the authentication process verify that this information is correct and the information is not used by another person. When these processes is implementing on internet it's called "Electronic authentication (e-authentication)". Electronic authentication is achieved by the following factors:

- **Knowledge** - something the user knows (e.g. user name, password, PIN, secret questions and answers, etc.);
- **Possession** - something the user has (e.g. Digital signature, smart card, etc.);
- **Be** - something the user is (e.g. biometric fingerprint, iris pattern, face recognition etc.); or - A combination of the above.

E-authentication service is implemented in different level. Here we give the different level of authentication service is that?

##### 4.4.1.1 Authentication Service Provision



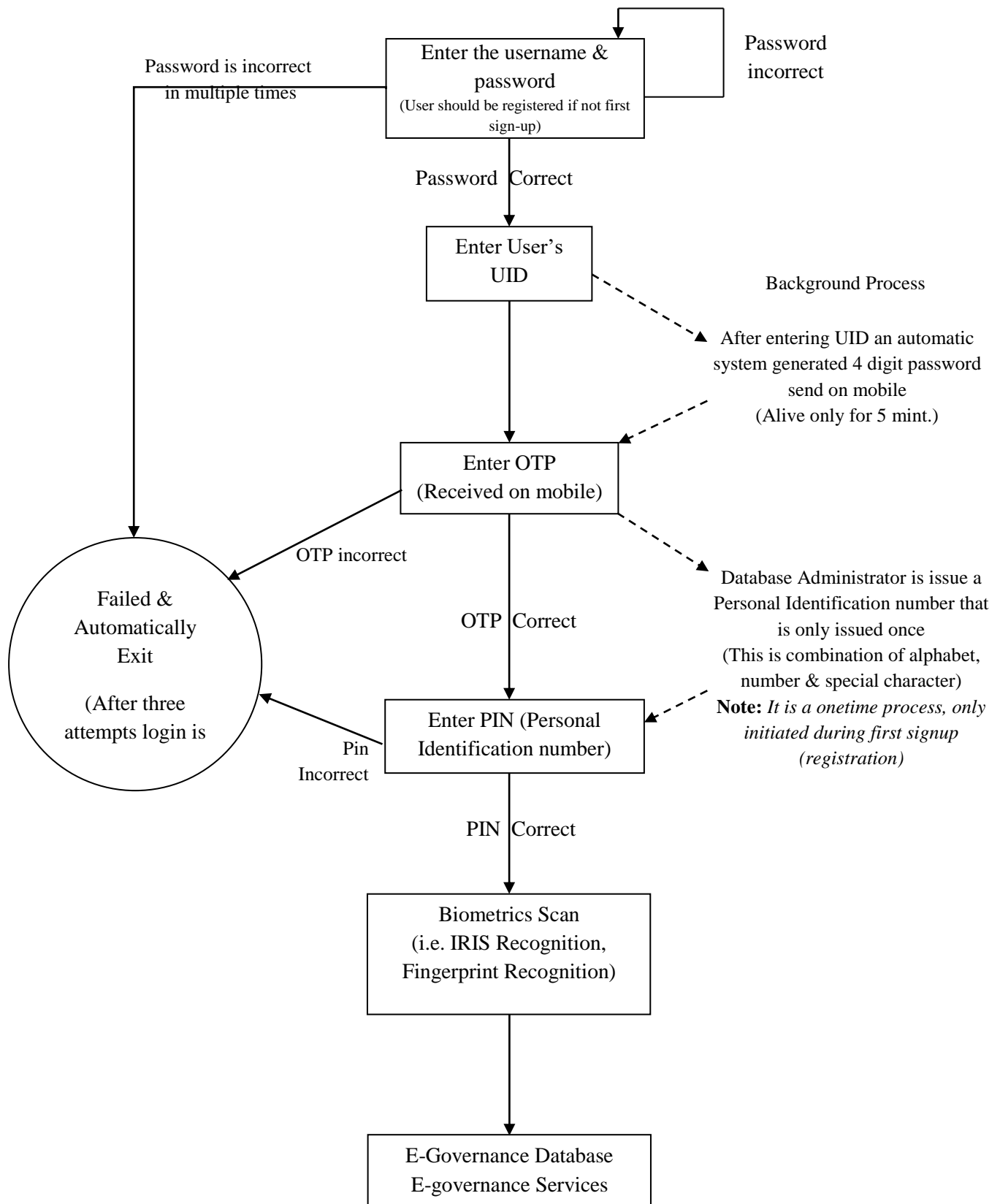
**Figure 4.6: Authentication Service Provision**

**Level 0:** This is the basic authentication mechanism using username and password. The user could be provided the capability of self-registration by which he/she can generate a username/password. He/she fill the self-registration form with the basic information also including the authenticated information like Aadhaar, PAN, Driving License, Rashan Card no etc. all this information helpful, if the user will forgot your username/password.

**Level 1:** At Level 1, a user will be able to prove her identity using OTP token along with his/her Unique Identification Card number (UID) credentials. The OTP will provide on his/her mobile phone no, this is entered at the time of registration of UID.

**Level 2:** At Level 2, the user would need to prove his/her identity through a hardware or software token (along with PIN). For this purpose, token would be a digital certificate/digital signature or a smart card or personal identification number (PIN) issued by the higher authority that would be required from the login.

**Level 3:** At Level 3, the user will prove his/her identity using biometrics authentication. This is the highest level of authentication security that would be available to a user. Biometrics based verification would be done in accordance with the Aadhaar authentication process.



**Figure 4.7: Data Flow of Authentication service provision**



#### 4.4.2. E-GOVERNANCE SERVICES

E-governance shell is providing the different type of services through our web-portal. So that government also has a responsibility for our web portal meaning that web-portal has required some service also like secure web-portal, data is stored in digitally so the confidentiality of data, data protection. Here we briefly describe all of responsibility of e-governance for the web-portal. E-governance services are show in figure 4.7 is here.

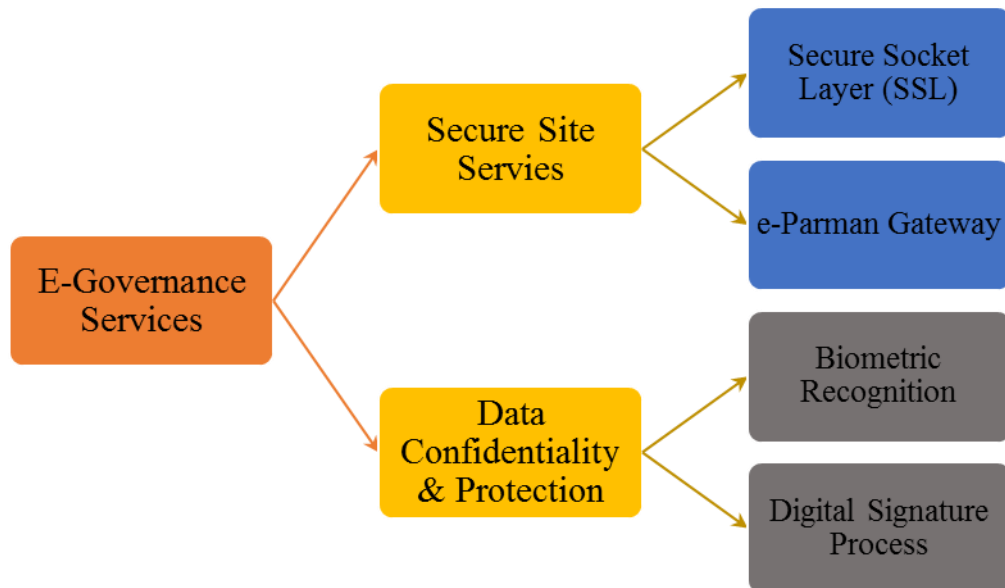


Figure 4.8: E-governance Services

##### 4.4.2.1. Secure Site Service

Secure site service also offers a range of security services like Distributed Denial of Service (DDoS) and cyber-threat reporting. It also works on SSL (Secure Socket Layer), PKI (Public Key Infrastructure), VeriSign Trust Seal and VeriSign Identification Protection (VIP) Service in 2010. VeriSign is the American company based in Reston, Virginia. VeriSign offer your agency the power to secure E-Government sites for safe information transfer, even for financial transactions.

**4.4.2.2.1 Secure Socket Layer (SSL)** – is an Internet protocol for secure exchange of information on the internet. It provides two basic security services: authentication and confidentiality. Logically it provides a secure pipe between the sender and receiver. It's developed in 1994, currently SSL comes in four versions: 2, 3, 3.1 and 4. The World Standard for Web security SSL4 technology is used to protect information transmitted over the Web with the ubiquitous HTTP protocol. SSL protects against site



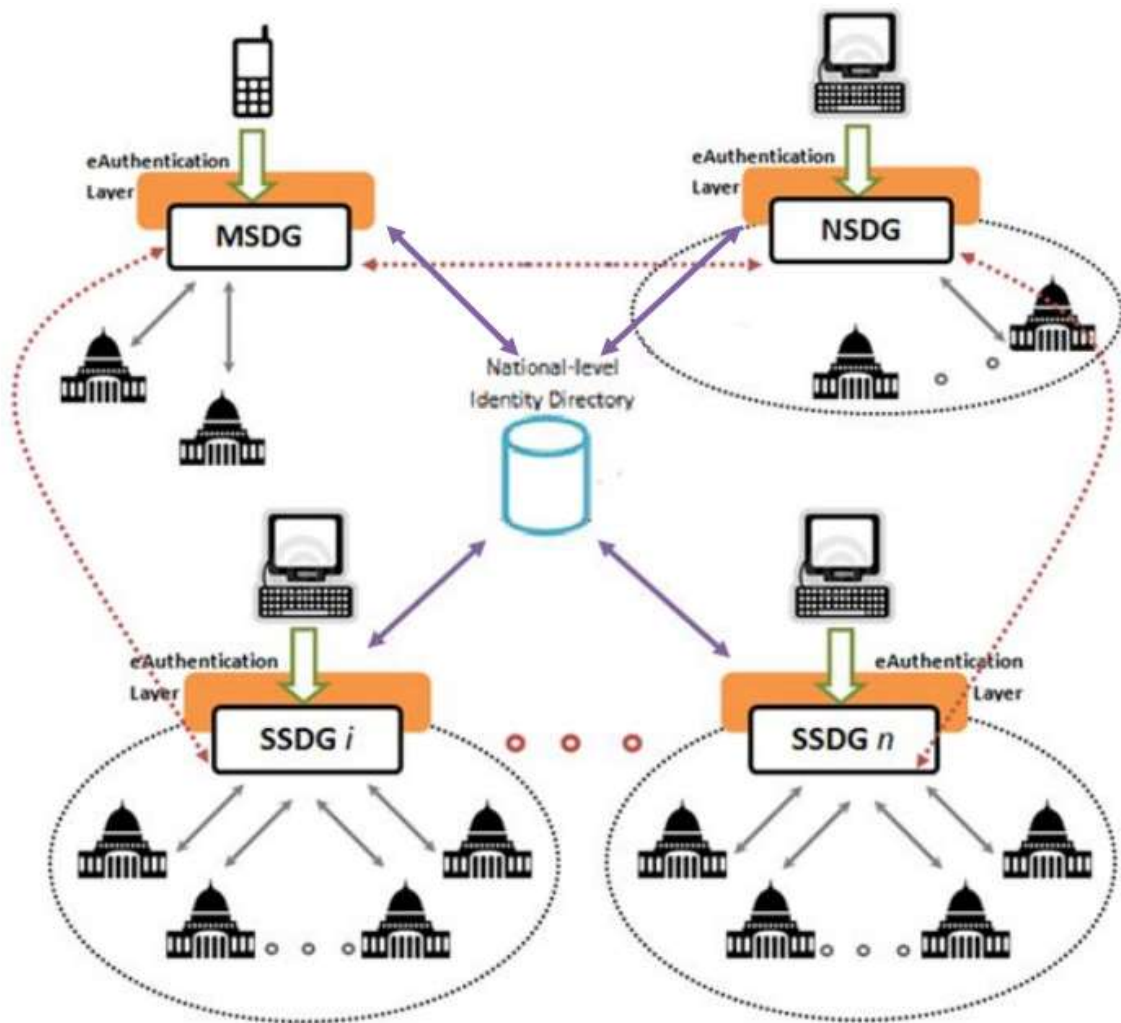
spoofing, data interception and tampering. Support for SSL is built into Web applications and server hardware. By powerful encryption through SSL Certificates on E-Government site servers with the confidence instilled, our system can immediately protect sensitive data transmitted between servers and other agencies, constituents, employees and e-government partners.

Currently e-governance web portals is working on the 46-bit SSL encryption but 128-bit SSL encryption is already working in other countries so if India should be used the 128-bit encryption the advantage of 128-bit SSL encryption and working is below.

**128-bit SSL Encryption** - The SSL Certificate is attached with web portal then this is highly secured from the attacker and secure for visitors. SSL protects our confidential information from the attacker and interception. 128 bit SSL encryption; this is the world strongest SSL encryption with both home and professional versions. This is developed for the Microsoft and Netscape browsers. At present 128-bit SSL encryption is used for large scale online business/trading, bank, health and insurance organizations. We have required to use one SSL certificate per domain name.

**4.4.2.2.2 e-Parmaan Gateway** – Under the National e-Governance Plan (NeGP), National and State e-Governance Service Delivery Gateways (NSDG/SSDG) have been created to ensure interoperability among autonomous and heterogeneous entities of the government at both central and state levels. NSDG and SSDG infrastructure acts as a standards-based messaging middleware between service access providers and government departments acting as service providers. Additionally, for mobile governance services, Mobile Service Delivery Gateway (MSDG) has been created that provides a government-wide shared infrastructure [54].

e-Parmaan Gateway shall leverage the middleware messaging infrastructure of NSDG, SSDG and MSDG to provide a convenient and secure way for the users to access government services via internet/mobile as well as for the government departments and agencies to assess the authenticity of the users [54]. The e-Parmaan Gateway shall be integrated with NSDG, SSDG and MSDG and shall act as a standard e-authentication mechanism between service access providers and the corresponding messaging middleware (NSDG, SSDG or MSDG). Figure depicts how this.



**Figure 4.9: The e-Parmaan Gateway [54]**

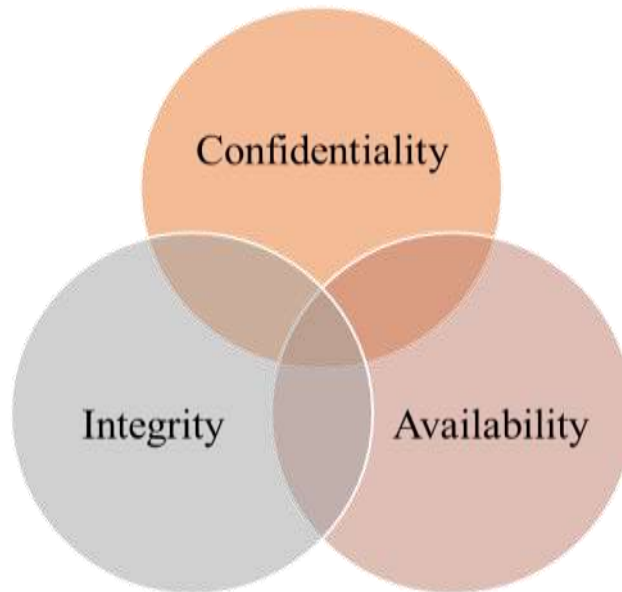
Integration shall be achieved. In order to leverage the NSDG, SSDG and MSDG infrastructure, the e-Pramaan Gateway will establish a centralised identity directory. E-Pramaan Gateway may incorporate new technologies, processes and authentication mechanisms in future [54].

#### **4.4.2.2 Data confidentiality & Protection**

Data Confidentiality is simply based on the three different but basic concept of security is that:

- **Confidentiality** – Confidentiality means the data is travel between the senders to receiver that time this is not accessed by other person. Confidentiality gets compromised if an unauthorized person is able to access information. Confidentiality is loss only in interception causes.
- **Integrity** – Integrity, when the senders send the information to indented receiver then in during the transmission this is not changed or modified by third person. *Integrity* is loss when the unauthorized user is made some modification or destruction in original information, this is loss by modification.

- **Availability** – In simply manner availability is that resources should be available to authorized parties at all times. Availability is loss only in interruption causes.

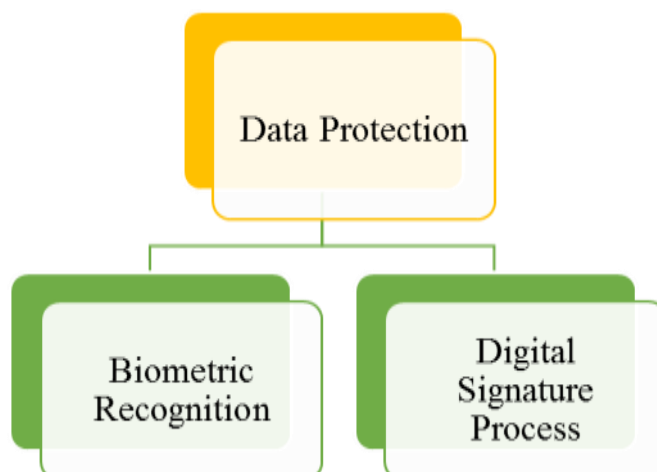


**Figure 4.10: Interconnection of Confidentiality, Integrity & Availability**

The Key law and standards for the data protection that apply to information governance includes, but is not limited to:

- The Data Protection Act 1998
- The Public Records Act 1958

The data protection should completed based on two approaches biometric recognition and digital signature process, these is show in the figure classification of data protection system.



**Figure 4.11: Classification of Data Protection System**

**4.4.2.2.1 Biometric Recognition** – This is a method or process to recognize a person with his/her verifying identity with help of behavioral or physiological characteristic. In physiological characteristic, there is checking of his/her fingerprint, face

recognition and IRIS recognition while in behavioral characteristics, dynamic signature verification, speaker verification, and keystroke dynamics are checked. UID and Indian governments is used the only physical characteristic, in which both IRIS recognition and Finger Print Recognition are included.

This is further classified in two different approaches, shown in the figure of categorisation of biometric recognition.

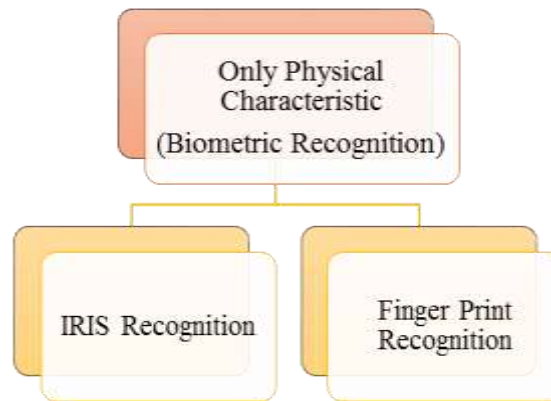


Figure 4.12: Categorisation of Biometric Recognition

#### A. IRIS Recognition

IRIS recognition is done for make the UID in India, it's a very difficult task for more then 100 billions people but the Indian government is almost done this task. So those governments easily implement iris authentication system in government offices/organizations. In present system IRIS recognition would be a high level of authorization. Every human's pupil structure is different. This type of security is most difficult for break. But this is required the special type of scanner here we shortly discuss how iris scanner scan the human's pupils. IRIS scanning process is completed in the four steps this is shown in figure:

- a) ***Outer iris inwards to pupil edge*** – Scanner reads firstly the human's pupil and mark the iris boundary that is in the pupil's boundary every human have different iris size it's unique.
- b) ***Plots distinct markings on iris*** – After that scanner plots the different distinct marking on the iris for making the unique shape of the iris.
- c) ***All data is stored*** – After plotting the marking on iris these plot marks within the iris is stored in the database.
- d) ***Data will compare*** – At last these is compare to other stored data for verify individual identities, each and every time the plotting is different.

#### HOW IRIS SCANNERS RECORD IDENTITIES

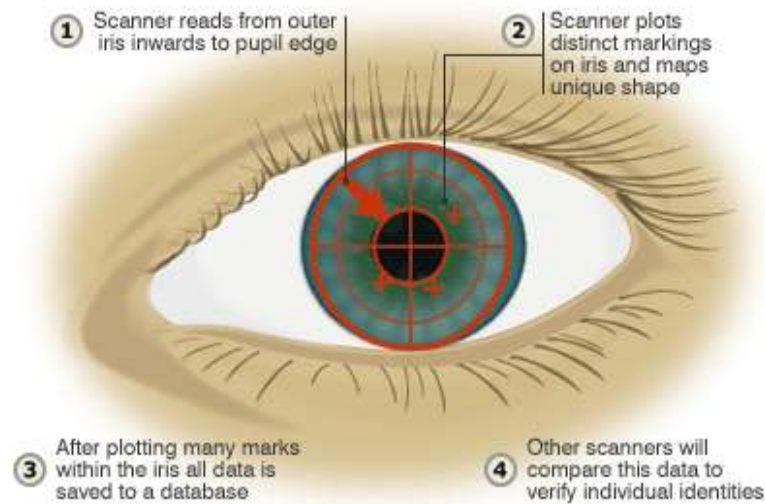


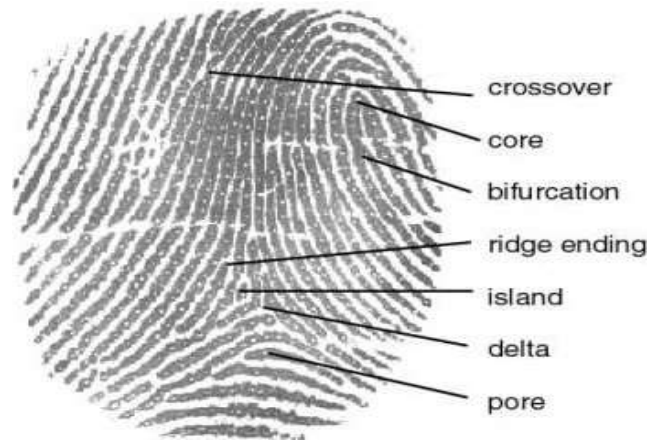
Figure 4.13: IRIS Recognition System

### B. Fingerprints Recognition

Fingerprint recognition also done in UID project not even a single figure but also stored all the ten figures in database. Fingerprint recognition is also count in high level of security system implementation but it is less secured as compared to the IRIS recognition because if attacker will have a user fingerprint then they easily use it. Here we also give the short discussion about the how fingerprint recognized by scanner. It's completed in seven different steps, this is show in figure:

- Crossover** – Into the first step identified the how many times two ridges cross each other. In the entire humans the ridges cross to each other is different numbers.
- Core** – After the identified the ridges cross to each other the scanner identify the center, center is that point where the ridges are starting the turn at 180° round; this is called the center of the core.
- Bifurcation** – Scanner identified the point where the ridges are start to separates or divided into the two different ridges, this point is bifurcation.
- Ridge ending** – Scanner will identify the end point of ridge and marks it and stored in the database.
- Island** – Scanner find the island in the finger print. This island is just the normal island means that small land in between the oceans. In the fingerprint island is small ridge between the two spaces. This makes the fingerprint unique. Scanner major the size of island and position of island in finger.
- Delta** – Scanner is identified the delta in fingerprint, delta is the space between ridges.

- g) **Pore** – Scanner at last identified or stored the human pore. Pore is that place where the two core ridge separate to each other.



**Figure 4.14: Fingerprint Recognition**

**4.4.2.2.2 Digital Signature** – Digital signature is an identification of a user to authorize as a intended user. Digital signature is issued by the certification authority (CA). when the user is once used the digital signature in message after that the document is not modified or the content of documents is not replaced. This can be used for send the message in encrypt or plan text format. This is done with the three different type features is that

- **Authentication** – Authentication mechanisms help to establish proof of identities. The authentication process ensures that that the origin of a electronic message or document is correctly identified. For instance, suppose that the sender will send a message to intended receiver but the message is read by third person during the transmission but he is not authorized to read it only the intended receiver is authorized to read it, this is called the authentication and read the message by third person it is called the *fabrication*.
- **Integrity** – when the content of message are changed after the sender sends it, but before it reaches the intended receiver, we say that the integrity of message is lost. If once the e-mail's content is digitally or electronically signed by the sender after the modification or changes will done by any other per until unless this is not modified by the intended receiver.
- **Non Repudiation** – Digital signatures ensure that the sender who has signed the information cannot at a later time deny having signed it.

Electronic Signature	Digital Signature
Simple Electronic method	Advanced Electronic Signature
Less Secure(tampered or altered)	More Secure
Digitized image of a handwritten signature, a symbol, voiceprint	Digested and encrypted form of original message
Does not use public key infrastructure technology	Based on Public Key Infrastructure (PKI) technology

**Table 4.1: Differences between Electronic Signature & Digital Signature**

#### **4.4.2.2.2.1. Legal Validity of Digital Signatures**

The Indian Information Technology Act 2000 (<http://www.mit.gov.in/content/information-technology-act>) came into effect from October 17, 2000. One of the primary objectives of the Information Technology Act of 2000 was to promote the use of Digital Signatures for authentication in e-commerce & e-Governance. Towards facilitating this, the office of Controller of Certifying Authorities (CCA) was set up in 2000. The CCA licenses Certifying Authorities (CAs) to issue Digital Signature Certificates (DSC) under the IT Act 2000. The standards and practices to be followed were defined in the Rules and Regulations under the Act and the Guidelines that are issued by CCA from time to time. The Root Certifying Authority of India (RCAI) was set up by the CCA to serve as the root of trust in the hierarchical Public Key Infrastructure (PKI) model that has been set up in the country. The RCAI with its self-signed Root Certificate issues Public Key Certificates to the licensed CAs and these licensed CAs in turn issue DSCs to end users.

According to amendment of IT Act Digital Signature (Section 3); provision in this section is user should authenticate the digital document with attached his/her digital signature. After that the document is placed in the digital envelop, that is crypto system hash function. Public key of the sender can only verify the digital record for any person who wants to access this digital document. Public key and private key both are the unique key for the each user.

Electronic Signature (Section 3A); Not with standing with the section 3, but some special provisions of subsection (2), sender should be authenticate all digital documents by digital signature or authentication technique which – (a) is consistent judge; and (b) may be identified in another agenda.

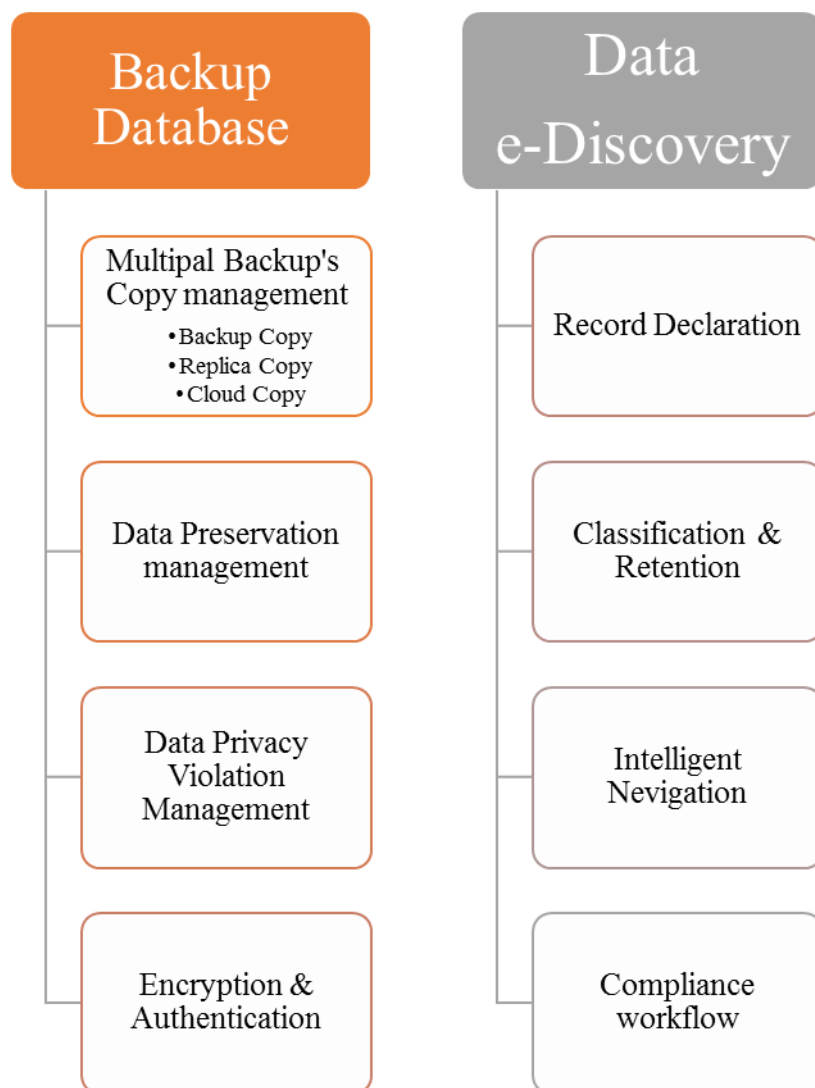
Digital/electronic signature or authentication process shall be reflecting on – (a) the signature design data or the authentication data both are not known by other person, that what information or data are used in it and how linked to the party; (b) the

signature design data or the authentication data both are under the control of the party or in other case may be certificate authority (CA) organization, not other person; (c) if any modification made in document after digitally sign, the signature should be noticeable; (d) if any modification made in the information after authentication by digital sign should be noticeable; (e) it fulfils such other conditions which may be prescribed.

#### 4.4.2.3. BACKUP & E-DISCOVERY FRAMEWORK

This framework is used for backup means the extra copy of all data that is sorted in database for the security regions like if main database is hacked by the attackers or crashed or any the disaster occurred so that the data is stored in the electronically form at another places in different format. This is described and show in the figure of backup and e-Dicoverry framework show in figure.

**Figure 4.14: Backup and e-Discovery framework**



**Figure 4.15: Backup and e-Discovery Framework**

##### 4.4.2.3.1. Backup



Backup is the process or method to save the data in another place with different format for the region of any disaster is occurred or database is hacked by the attackers. Backup is done with the different level is...

#### **4.4.2.3.1.1. Multiple backup's management**

Backup should be save in different copies if one copy is crashed or damage then other copy data would be used for restored and saved the data and they are stored in different places.

**4.4.2.3.2.1. Backup copy** – Refers to a copy of data that may be used to restore the original in the event the latter is lost or damaged beyond repair. Backup copy is made through the duplicate database. It is stored in the different forms like: optical disk, hard disk, magnetic disk etc. backup is mainly two types: cold & hot backup. Cold backup is directly stored in the other storage device and that is not modified by the user it's directly export in the database. Hot backup in which the online images take and that is stored in the backup devices. Backup copy is made in different types: incremental backup, binary backup, encrypted backup, automated database duplication etc.

**4.4.2.3.2.1. Replica copy** – Refers to make a duplicate database of the original with the different location or different network, or in different time zone for the user's availability. Replica is generated at the time of database created. In the database more than one replica is generated with the different locations. Replica is generated by the help of triggers. When the trigger is active they automatically generated the replica copy of original database in which each and every time the whole database copy is generated and last stored copy is auto replaced the new one. Using replicas reduces the network traffic because the user is not need to connect the central server database it's connect to local server database that is the replica of original database and make the changes, these changes is made automatically in original database, when all replicas is connect with original database.

**4.4.2.3.2.1. Cloud copy** – Data should be saved as backup in the cloud. Cloud means the data is shared or stored in the other servers and will be accessed in entire world. Cloud is further classified in two part public cloud and private cloud, but the government data is most sensitive data so that it is stored private cloud and accessed by the authorized person.

Public cloud is open access means that each and every person is easily access.

#### **4.4.2.3.1.2. Data preservation management**

This is the process for stored all the information or data. In preservation, preserve a copy of all the data that is stored in the database, regularly after the four month in every year (quartile). This storage is not for the disaster policy. The media in which is these preservation made, is not available after complete the process. It's done for taking the archive of the database, archive means that it takes in separate storage media and retained for long periods. Archive is not used actively. This is stored in mainly three different type is: XML, text and/or binary documents, plus metadata. The type is not under user control.

#### **4.4.2.3.1.3. Data privacy violation management**

Privacy issues by identifying and supervising key information entities. Entities include the use of unique identity number, credit card number or predefine patterns that are quickly recognized. That is also managed with workflow to key security and reduced individuals information risk.

#### **4.4.2.3.1.4. Encryption & authentication**

Ensures every record object managed is uniquely identified and authenticated using specific algorithms. Security is enhanced whether stored on-premise or pushed across to the cloud by purposed four level of security and five level of encryption that is certified and authenticated to worldwide standards.

#### **4.4.2.3.2. e-Discovery**

E-Discovery gives the power to user to make the search easy or efficient. It also takes the classified record. It does also improve with the user compliance.

##### **4.4.2.3.2.1. Record declaration**

It is help out to information shearing and collaboration of each and every person data. If the state government is declare the data of all persons and share with all central government then the data duplication is minimal and the particular user is easily to search or identified or if all state government share all the document with other state government portal then its very easy for all person to access these data and transparency of government work is improved.

##### **4.4.2.3.2.2. Classification & retention**

Discovery of any data make is easy and comfortable if all the data is classified, government should be make the different class like e-government projects, government future strategy, security issues etc. so specific groupings of records is identified by tags or metadata ascertained for the method of acquisition are aligned to flexible policies for retention and disposition.

#### **4.4.2.3.2.3. Intelligent navigation**

Is enabled through a unified central portal. Customizable to the needs of different users with specific capabilities that encourage the navigators.

#### **4.4.2.3.2.4. Compliance workflow**

Government should be workflow on the user's compliance regularly for improving the services. If government is strictly flow and solve the compliance of user they easy to maintain all the data and easy to serve all information from government to user or vice-versa.

**RESULT & CONCLUSION**

---

**5.1 Research Findings**

Cyber security is a typical task to do without a proper framework i.e. no cyber security can be done without having a predefined methodology or a step by step framework to get the end results. There is wide range of different types of cyber security today. Solution of each security requires a very complicated task.

Many cyber security frameworks are proposed to deal with it. A sequential flow technique is proposed in countless frameworks. Many of the existing frameworks can be seen to build upon each other by extending earlier approaches with the aim of becoming more complete and robust. Many of the digital authorization processes have been developed either by traditional encryption scientists focusing on robust technique handling or by technologists focusing on digital authentication assurance, making it difficult for law enforcement practitioners to understand and apply.

The proposed security and authorization framework is more convenient as compare to the exiting one. This provides many framework activities for security enhance with exiting facilities which helps to reduce uncertainty in processing. Every step is well defined so every government web portal is framed in proper way. The authorization part has been done in every step so as to get the appropriate result. The data collected is more precise and accurate as it is refined at e-discovery step. Main concern for the security enhancement is on the flow of information of the framework and then the authentication planning along with UID's Biometric recognition. The proposed framework has helped to improve existing regulatory tools and mechanisms to minimize risks/attacks. It has helped to provide a systematic approach for storing citizen information and its implementation which will significantly reduce the costs and time of an internal and external implementation.

The framework should be implementing and apply to solve a real time web portal of e-governance in INDIA. The framework has been solved the problem of security and authentication of user and backup and e-discovery of information on the e-governance web portal of INDIA.

**5.2 Limitations of the Research**

The major limitation of existing web security framework is that it refers only to the

registration and OTP (One Time Password) part of an authorization and issues such as the exchange of information, backup of data and intelligent search for user/government information are not addressed.

Also the proposed framework have 3 sub framework with sub phases, which give the advantage of more secure login and authorization of database with a time consuming job and hence delay in finding the information. Each sub-category added to the framework has made it more cumbersome to use.

One obvious area not touched upon in this framework is, the chain of risk management. Of course this is an important facet of any security enhance work. This framework assumes that a strong chain of risk management will be maintained throughout the duration of the security implementation. The absence of it on the model above makes no presumptions that it is not important, only that it is implied in any discussion of authorization.

Also the citizen's data collection strategies have been ignored.

### **5.3 Conclusion**

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 is exponentially increased due to imbalance in augmented growth of internet & less in awareness of security. The risks of security enhancement are very real and too threatening to be ignored. Every franchisor and licensor, indeed every business owner, Internet service providers, domain name registries, universities, law enforcement agencies, and other cross-industry stakeholders has to face up to their vulnerability and do something about it.

Hitherto a good starting has begun in 2006 & 2008 by endorsement of I.T. Act and amendments. Presently an organized and structured framework to deal with required security. At the very least, every government must conduct a professional analysis of their cyber security and cyber risk; engage in a preventive plan to minimize the legal responsibility; insure against losses to the greatest extent possible; and implement and promote a well-thought out security policy.

A new framework of e-governance security enhancement using UID has been described. The inclusion of information flows in this model, as well as the backup and intelligent search activities, makes it more complete than other frameworks. This framework has various sub frameworks as: Registration & Authentication framework, e-governance service delivery framework and framework for backup and e-Discovery.

It provides a basis for the development of techniques and especially tools to support the work of authorization. The viability and applicability of the framework now needs to be tested in different government, organizational web portals.

This framework can be applied on almost all types of authentication. This process framework does well at providing a general framework that can be applied to a range of security. This framework also shows the amount of effort that needs to be dedicated to properly authenticate a digital user.

The framework defines the different roles for technical. Each sub framework of this framework allows to develop more technical requirements and for the interaction between physical and digital user/person to be identified. Collection of digital identity from cross geographically placed servers is important in case of cyber and electronic transaction and backup of confidential information. It is therefore important that countries sign a Memorandum of Understanding to share information related to high-tech countries.







## **Annexure – I**

---

Important amendments to the provisions of the Citizenship Act, 1955 Section 14A

- 1) The Central Government may compulsorily register every citizen of India and issue national identity card to him.
- 2) The Central Government may maintain a National Register of Indian Citizens and for that purpose establish a National Registration Authority.
- 3) On and from the date of commencement of the Citizenship (Amendment) Act, 2003, the Registrar General, India, appointed under sub-section (1) of section 3 of the Registration of Births and Deaths Act, 1969 shall act as the National Registration Authority and he shall function as the Registrar General of Citizen Registration.
- 4) The Central Government may appoint such other officers and staff as may be required to assist the Registrar General of Citizen Registration in discharging his functions and responsibilities.
- 5) The procedure to be followed in compulsory registration of the citizens of India shall be such as may be prescribed.

In sub-section(2) of section 18 (ia) has been inserted after clause (i) the procedure to be followed in compulsory registration of the citizens of India under sub-section (5) of section 14A;

In sub-section (3) of section 18 the following proviso has been inserted “PROVIDED that any rule made in respect of a matter specified in clause (ia) of sub-section (2) may provide that a breach thereof shall be punishable with imprisonment for a term which may extend to three months, or with fine which may extend to five thousand rupees, or with both”.

## Annexure – II

### Policy on Open Standards for e-Governance

---

Government of India  
Ministry of Communications & Information Technology  
Department of Information Technology  
**Policy on Open Standards for e-Governance**

Effective Date : This Policy is effective from the date of notification

1. **Data Archival** – Data Archival is the long-term storage of data which is less frequently used or no longer in active use; the archived data should be retrievable for subsequent usage/reference whenever it is needed.
2. **Designated Body** – An agency appointed by GOI to (i) consider and recommend the selection of additional Open Standard in an Area (ii) give recommendations if multiple Open Standards are available in an Area with equal score on desirable characteristic and (iii) to review Interim Standards to check if it qualifies for adoption as Open Standards or for replacement with alternate Open Standards in that Area (iii) initiate action for formulation of Interim Standard in a situation where no standards are available to meet functional requirements for an Area.
3. **Domain** – A sub-category under an Information Technology field is Domain; specific purpose with in a “Domain” is known as “Area”. For example, “Document type for Web publishing content” is one Area under the “Presentation” domain.
4. **E-Governance** – A procedural approach in which the Government and its citizens, businesses, and other arms of government are able to transact all their activities or at least majority of activities using Information and Communication Technology tools.
5. **Essential Claims** – All claims in a patent that are necessary for implementation of the Recommendation
6. **FRAND/RAND An abbreviation** – for (Fair) Reasonable And Non-Discriminatory, is a phrase that defines a basic set of minimal terms that a patent holder is obliged to offer (such as granting a license that is world-wide, non-exclusive, perpetual, reasonable, and non- discriminatory, etc.) and leaves all other non-specified terms to negotiations between the patent holder and the implementer seeking a license
7. **Functional Requirement** – A function is described as a set of inputs, the behavior, and outputs in a specific Area. A functional requirement describes the functionality that the system is expected to execute; it may be calculations, technical details, data manipulation, processing, any other specific functionality supposed to be accomplished in the specific Area. For example, “Loss-less compression raster image” is an Area under “Presentation Domain” whose Functional Requirement is an image format with compression but without any loss of quality while doing repeated editing. Whereas “Lossy compression raster image” is another Area under “Presentation Domain”, whose Functional Requirement is an image format with high compression and small size by



8. **G2B** A set of services exchanged between government and the business community.
9. **G2C** A set of services exchanged between government and the citizen.
10. **G2E** A set of services exchanged between government and government employees.
11. **G2G** A set of services exchanged between government agencies.
12. **Interim Standard** A standard temporarily adopted as per the process defined in any one of the sections “Non-availability of Open Standard which meets all Mandatory Characteristics” and “Non-availability of Standards which meets functional requirements” of the Policy on Open Standards.

The Interim Standards would be reviewed regularly by Designated body to check if any of the Interim Standard (i) qualifies to be adopted as an Open Standard or (ii) Any other Standard has been identified as an Open Standard to replace this Interim standard in the Area.

13. **Identified Standard** A standard which meets maximal essential functional requirements for an Area of e-Governance systems.
14. **Interface** A boundary across which two independent systems meet and act on or communicate with each other.
15. **Legacy System** An old method, technology, computer system, or application program that continues to be used, typically because it still functions for the users' needs, even though newer technology or more efficient methods of performing a task are now available.
16. **Maturity** A Standard is considered mature if different implementations, proprietary/open, are available widely adopted and have been stable for some time
17. **New version of Legacy System** The legacy system which has undergone a major version change due to re-engineering like functional changes, architectural changes, technology changes, change in storage mechanism, design implementation changes.

18. **Not-for-profit** Not-for-profit organisations include major internationally recognized Standards bodies such as the IETF, ISO, IEC, W3C, OASIS including any agency recognized or designated by the GoI as such for the purpose of Open Standards.
19. **Open Standard** A standard which meets all mandatory characteristics laid down in the Policy.
20. **Royalty** A stream of payments for use of a certain type of asset/technology, most typically an Intellectual Property Right (IPR).
21. **Royalty-Free (RF)** A Royalty Free (RF) Standard is a Standard whose license is not conditioned on any payment of royalties, fees and other monetary considerations on its use in an implementation. The RF License is also subject to the following conditions:
- a. It shall be available worldwide on non-exclusive basis for the life time of the standard.
  - b. It shall extend to all Essential Claims owned or controlled by the participating patent holders ( i.e., those developing the standard).
  - c. It could be conditioned on a grant of a reciprocal RF license.
  - d. It shall not impose any further conditions or restrictions on the use of any technology, intellectual property rights, or other restrictions on behaviour of the licensee, but may include reasonable, customary terms like relating to operation or maintenance of the license relationship such as the following: choice of law and dispute resolution.
22. **Specifications document** A document that consists of a set of concise statements of requirements for a system.
23. **Standard** A specification, method, process or practice for a system that is both widely used and accepted or is sanctioned by a Standards Organization.
24. **System** A group of interacting, interrelated, or interdependent elements forming a complex whole. Information System is a combination of people, hardware, software, communication devices, network and data resources that processes (can be storing, retrieving, transforming information) data and information for a specific purpose.

**REFERENCES**

1. Hanna, N.K., *Why National Strategies are needed for ICT-Enabled Development*, I.S.W. PAPERS, Editor. 2003. p. 1-47.
2. CIO, H.K.O.o.G., *Digital 21 Strategy – Sustainability and Opportunities*. 2004, Commerce, Industry and Technology Bureau: Hong Kong.
3. 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.
4. IDA, *Innovation, Integration and Internationalization – Report by iN2015 Steering Committee*. 2006, Information communication Development Authority: Singapore.
5. Headquarters, I.S., *e-Japan Strategy*. January 22, 2001 Prime Minister of Japan and His Cabinet.
6. Headquarters, I.S., *e-Japan Strategy II*, I. Technology, Editor. 2003: Japan.
7. *e-Korea Vision 2006 – Third Master Plan for Informatization Promotion (2002 - 2006)*, M.o.I.a. Communication, Editor. 2002, Government Press: Korea.
8. Technology, D.o.I., *e-governance 2012 Strategy*, I. Technology, Editor. 2010.
9. A. Ojo, M.S., and T. Janowski, *Macao IT Strategy for 2010 - 2020: Process, Scenarios, Strategies and Governance*. 2009, Center for Electronic Governance, UNU-IIST: Macao.
10. UN, *United Nations E-Government Survey 2012*, E.S. Affairs, Editor. 2012. p. 160.
11. Guido, B., *United Nations e-Government Survey 2008: From e-Government to Connected Governance* E.a.S. Affairs, Editor. 2008, United Nations publication New York. p. 1-246.
12. Yong, J.S., *E-Government in Asia Enabling Public Service Innovation in the 21st Century* 2003: Times Media. 421.

13. DAVIS, J., *Corruption in Public Service Delivery: Experience from South Asia's Water and Sanitation Sector*. Elsevier, 2004. **32**(1): p. 53-71.
14. [http://www.indg.in/india/about-c-dac/view?set\\_language=en](http://www.indg.in/india/about-c-dac/view?set_language=en) 27/07/2013].
15. Bharat Maheshwari, V.K., Uma Kumar, Vedmani Sharan, *E-Government Portal Effectiveness: Managerial Considerations for Design and Development*. Computer Society of India, 2007: p. 12.
16. Holmes, D., *eGov: eBusiness Strategies for Government*. 2001: London : Nicholas Brealey. 330.
17. Joseph S. Jr. Nye, J.S.N., John D. Donahue, *Governance in a Globalizing World*. 2000: Brookings Institution Press\.
18. DOIT. *National e-Governance Plan*. 22/05/2013].
19. DOIT. <http://deity.gov.in/content/e-governance#>
20. DOIT. *National Portal of India*. 17/05.2013].
21. Chopra, K. and W.A. Wallace, *Trust in Electronic Environments*, in *Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03) - Track 9 - Volume 9*. 2003, IEEE Computer Society. p. 331.1.
22. Unit, E.I., *E-Readiness rankings 2009: The usage imperative A report from Economist intelligence unit*. 2009, The IBM Institute: LONDON.
23. PRASAD, K., *E-GOVERNANCE POLICY FOR MODERNIZING GOVERNMENT THROUGH DIGITAL DEMOCRACY IN INDIA* JOURNAL OF INFORMATION POLICY, 2002. **2**: p. 21.
24. India, g.o., *Guide on Right to Information Act, 2005*, by Government of India, D.o.P. Training, Editor, Government Press: Delhi.
25. K.F.Wong, M.K.W.T., C.H.Cheng, *E-government — A Web Services framework*. Journal of Information Privacy & Security, 2006. **2**(2): p. 21.
26. Joseph, R.C. and D.P. Kitlan, *Key Issues in E-Government and Public Administration*, in *Handbook of Research on Public Information Technology*. 2008, IGI Global. p. 1-11.
27. Kallol, B., *Factors Contributing to Global Digital Divide: Some Empirical Results*. Journal of Global Information Technology Management, 2005. **8**(3): p. 47.
28. Servon, L., *Bridging the digital divide: technology, community, and public policy*. 2002: {Wiley-Blackwell}.

29. <http://www.UIDAI.gov.in>. 08/06/2013].
30. <http://expertnet.wikispaces.com/Getting+Started>. 19/05/2013].
31. [http://www.mgs.gov.on.ca/en/IAndIT/STEL02\\_046927.html](http://www.mgs.gov.on.ca/en/IAndIT/STEL02_046927.html). 3/5/2013].
32. <http://www.ciw.ca/en/GetInvolved.aspx>. 09/06/2013].
33. *A national framework for greater citizen engagement*, M.o. Justics, Editor. 2008. p. 25.
34. <http://digital.cabinetoffice.gov.uk/projects/>. 27/04/2013].
35. [www.data.gov.uk](http://www.data.gov.uk). 19/05/2013].
36. Vergara, V., *A glance at participatory budgeting in Porto Alegre and Entebbe and operational implications for the World Bank*. 2002, <http://siteresources.worldbank.org/INTEMPowerment/Resources/486312-1095970750368/529763-1095971096030/vergara.pdf>. p. 11.
37. <http://www.towardq2.qld.gov.au/tomorrow/index.aspx>. 21/05/2013].
38. Jeong, C.H.I., *Fundamental of development administration*. 2007, Scholar: Puchong.
39. [http://portal.unesco.org/ci/en/ev.php-URL\\_ID=4404&URL\\_DO=DO\\_TOPIC&URL\\_SECTION=201.html](http://portal.unesco.org/ci/en/ev.php-URL_ID=4404&URL_DO=DO_TOPIC&URL_SECTION=201.html). 07/06/2013].
40. Clift, S. (2003) *E-Democracy, E-Governance and Public Net-Work*.
41. Europe, C. <http://www.coe.int/T/E/Com/Files/Themes/e-voting/definition.asp>. 17/05/2013].
42. Backus, M., *E-Governance and Developing Countries* 2001. p. 51.
43. Kettl, D.F., *The Transformation of Governance: Public administration for the twenty-first century America*. Paperback. 2001, Baltimore and London: Johns Hopkins University Press. 204.
44. [www.worldbank.org](http://www.worldbank.org). 13/07/2013].
45. Sharma, S.S., *Assessing E-government Implementations*. Electronic Government Journal, 2004. 1(2).
46. Sharma, S.S., *An E-Government Services Framework*. 2006. p. 376-378.
47. Sharma, S.K. and J.N. Gupta, *Building Blocks of an E-Government: A Framework*. 2003, IGI Global. p. 34-48.
48. [www.unpan.org](http://www.unpan.org). 19/07/2013].
49. [www.gbde.org](http://www.gbde.org). 09/08/2013].
50. [http://www.tatasteel.com/technologyupdate/km/km\\_basics.htm](http://www.tatasteel.com/technologyupdate/km/km_basics.htm). 04/06/2013].



51. [www.pacificcouncil.org](http://www.pacificcouncil.org). 01/08/2013].
52. Frage, E. *Trends in e-Government: How to Plan, Design, and Measure e-Government*. in *Government Management Information Sciences (GMIS) Conference*. 2002. Santa Fe, New Mexico, U.S.A.
53. Leitner, C., *eGovernment in Europe: The State of Affairs*. 2003, Atlanta, Belgium. 68.
54. Technology, M.o.C.a.I., *e-Pramaan: Framework for e-Authentication I*. Technology, Editor. 2012, Government Press. p. 18.
55. *Policy on Open Standards in eGovernance*, DOIT, Editor. 2010. p. 13.
56. India, G.o., *Gazette Vide GSR No. 937(E)*. 2003, Government Press.