Development of Privacy Protecting Identity Management System for E-Government in India

Aparajita Pandey
Astt. Professor, BIT(Mesra), Jaipur Campus
Email: aparajitasp@rediffmail.com
Dr. Jatinderkumar R. Saini
Director (I/C) & Associate Professor,
Narmada College of Computer Application, Bharuch, Gujarat, India
saini_expert@yahoo.com

----------**ABSTRACT**----------

From the beginning of modern governance and structured commerce, both public and private service agencies across the country typically require proof of identity before providing services to individuals. In the online world it becomes the responsibility of the government to ensure the security and privacy of the citizens using the Identity Management Systems of the government. In this paper a privacy protecting identity management system is proposed for use in e-government.

Keywords-**Identity Management, Online Identity, Privacy, e-government, Smart card**

I. INTRODUCTION

1.1 GOOD E-GOVERNANCE

E-government can be described as comprising all endeavors to *make government workable* and *accessible in electronic form*. 'E-Government' therefore has a back-office where work inside government is to be handled electronically, and a front-office, which relates to the communication between individual citizens , the business community or other public bodies etc. It is not enough to just electronify the traditional ways and means of operating in government – successful e-government requires re-engineering administrative processes to a considerable degree in order to fully profit from the possibilities of applying IT. An important item in striving for good governance is the accessibility of government functions. For citizens and businesses as well as Government authorities' efficiency of government services depends on the easy availability of information and on easy and reliable access to communication facilities. Electronic communication through internet is the prime solution according to the possibilities of today´s information technology. Special security features must be provided when used for legally relevant communications.

1.2 IDENTITY MANAGEMENT

Identity Management can be described as the policies, rules and processes and systems involved in ensuring that only known, authorized identities gain access to networks and systems and the information contained therein.[1].There are different models of Identity Management techniques, The Single Sign On (SSO) Model, The Centralized model and the Federated Model. [2].The different IdM models have some advantages and disadvantages which are discussed in the paper "Online Identity Management Techniques: Identification and Analysis of Flaws and Standard Methods" [3].The challenges faced in implementing the Federated Online IdM techniques are discussed paper "An Investigation of Challenges to Online Federated Identity Management Systems"[4]

II. DIFFERENCES BETWEEN ONLINE AND OFFLINE IDENTITY MANAGEMENT SYSTEMS

In the online world large amount of information is collected and interconnected as compared to offline mode. This benefits the government and the citizens but it creates several risks that did not exist in paper based systems. In E-governance the accountabilities and responsibilities are not clear; this makes it difficult for the citizens to receive compensation. For example if a government online portal provides single sign on (SSO) services for several agencies, it is not clear about which agency is responsible if the system fails. Responsibilities and accountability can fall under several parts of government hierarchy, the ministers responsible for a particular agency, the web –masters who designed the portal and the officials who approve or administer it.[5]

III. IDENTITY MANAGEMENT IN INDIA

India is one of the leading IT services providers to the businesses across the world with US$60 billion outsourcing industry [6].With the increase in the number of Internet users and increased penetration of technology in modern India's individual, the exposure to the e-threats and privacy breach has increased as well. These threats can cause potential damages to financial, social, and personal interests of the individuals, e.g. targeted advertising. The last few years also witnessed conceptualization of countrywide projects such as UID (Aadhar) and NATGRID (National Intelligence Grid). Increasingly services such as banking,

insurance, and telecom are introducing Information Technology (IT) enabled services increasing the purview of IT on life. Various studies in the past [7], [8] have shown Indian population to be less sensitive to the privacy in comparison to countries of the world, significantly because of the collectivistic nature of Indian society.[9] Another aspiring project, NATGRID by the government faced significant opposition due to the involved threats to the privacy of the Indian individuals.

Governments are quickly developing and transforming national policies for identity management. If done well the rewards are incredible; if done poorly, policy failure will be certain. Comprehensive identity policies involve creating or adapting schemes for the collection and processing of individual–specific data that will be shared across services, both within and beyond government, often for a variety of purposes. The range of bodies involved in such policy developments is widespread, raising important issues both for the government led implementation of such policies and for academics to study and engage the policy discussions as they take place. In an age of 'identity management', when government seeks to define and to control identity, and the individual is overwhelmed by fears of identity theft and the all-seeing, intrusive state.[10]

IV. WORK FLOW PROCESS IN E-GOVERNMENT

E-Government system aims at comprehensiveness. It includes the search for information, the bringing in applications, the working out of decisions and finally the delivery of decisions to the citizen(s) involved. Things are handled electronically – in the back office as well as in the front office.

4.1 BACK OFFICE

Concerning the back-office dimension of e-government offices work should be done, exclusively electronically with the possibility of direct electronic exchange of documents inside and between all ministries in an especially secure system. Authenticity can be guaranteed by means of digital signatures.

4.1 FRONT OFFICE

This paper shall, however, mainly deal with front office' aspects of e-Government, that is the way how communications between government bodies and their 'customers' take place. For efficient e-government it is essential that procedures are pre-determined in such ways that it is not necessary to resort to other, additional means of communication (e.g. telephone, personal appearance before the authorities etc). A structured electronic dialogue is best provided for by web-based communication. That is why the proposed e-government system entirely relies on web communication.

V. PROPOSED SOLUTION FOR IDENTITY MANAGEMENT IN E-GOVERNMENT

The proposed solution for IdM in India achieves interoperability of e-Government Systems. Interoperability and cooperation can be regarded as enablers of the integration of e-Government applications. A prerequisite, the ultimate goal of any integrated, collaborating systems and organizations is the sharing of information or data. It is self-evident that such sharing is only possible when the identification of the entities the data describes is well understood. This research is focused on the identification and related data protection issues.

It is worth mentioning that a person can have more than one identifier – depending on the roles he/she or it plays in societal, economic, technical and public contexts. At this point, it is also justified to talk of more than one identity the same person bears. This multiplicity makes necessary the definition of technical and organizational measures and processes to handle it, or in one term: Identity Management. There is a strong technical prejudice in the research and development of identity management related concepts. Notions like digital signatures, authentication, smart cards, identity federation, which adds the concept of anonymous identifiers/identities, require and encompass advanced technical approaches for handling digital identities. All countries we have studied use such "traditional" identifiers for natural and legal persons.[11].The most fundamental difference between these systems is the number of different identifiers used by public administrations. There might be a single, national and "all-purpose" identifier1 single identification number or **SIN** for e.g. SSN in US & Aadhaar in India), used by all administrations, and possibly by economy and in private contexts. Or there might be several, so called sector-specific and independent identifiers – like **PAN** or driving license or actually a combination of these, although this could be regarded as being contradictory. The co-existence of a so-called single and further identifiers could be explained either as a transitional phenomenon, because the implementation of a national identifier takes time. This means that single in this case means almost single and further identifiers exist only in different departments. We can summarize these definitions as in Table no.1

Table 1 Types of Identifiers

Type of identifier	Characteristics of Systems using such identifiers	Number of personal identifiers
SIN	Single, multipurpose ID used in all administrative contexts	1
Department Specific ID	One or several IDs used in different administrative contexts	≥1

In our proposed solution, we will use a new technology based identification system .The system, on the one hand, takes into account the strong, history-related data protection concerns that prevail in the country. On the other hand, it provides an efficient way of identification management and serves as an enabler for e- Government solutions, treating also authentication related issues like digital signature, public key infrastructure (PKI), etc.

All the citizens are registered in the National Population Register (NPR) and have a registration number. From this number, a so-called "fundamental identification number" (fPIN) is derived, using a strong encryption algorithm. This number is stored on the new electronic citizen card. When used in contacts with public administrations, the fPIN serves together with a department specific tag as input for the encryption algorithm for "department specific pins" (dsPINs) for the exclusive usage in the corresponding sector. (e.g., IT Dept).

. This means that in practice, each department must use different identifiers, hence the combination of the central identity management and its advantages with a strong "SILO" approach making impossible uncontrolled data sharing outside well-defined zones. Fig.1. gives a simplified overview of the system.

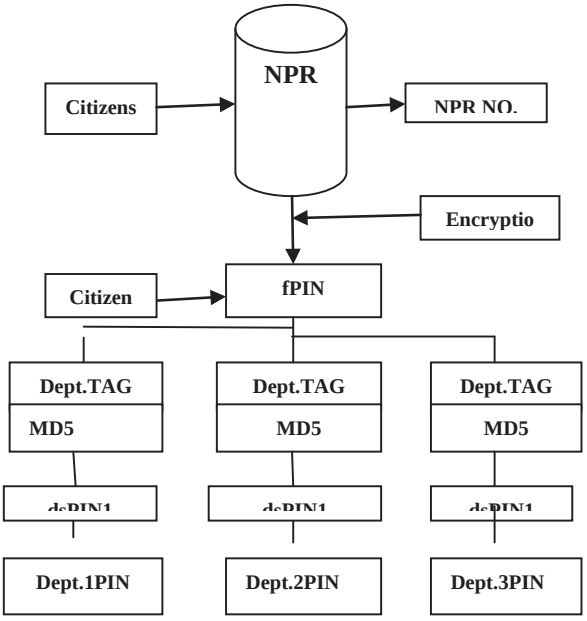


Fig.1 Proposed Solution

India established its National Population Register [NPR) in 2010. Every citizen in India is registered in NPR and is assigned a unique personal identification number [PIN) the so called NPR-number. As a result, every person in India will get a unique PIN. The NPR is a register of usual residents. The data collected in NPR after authentication is sent to UIDAI for de-duplication and issue of Aadhaar Number. Thus the register contains three elements of data - [i) demographic data, [ii) biometric data and [iii) the Aadhaar [UlD Number). [12]

For privacy reasons the base register numbers, the NPR number is not used as the unique identification number in our proposed solution. Especially the NPR number is never used for this purpose. Instead, a specially derived number called the fundamental PIN [fPIN) is introduced as the base unique identifier for identification in an electronic transaction.

The central governmental department, say fPIN Registration Authority, should be the only department allowed to create these fPINs. The creation of fPIN is done by adding a secret seed-value to the base number (NPR number) and by applying a cryptographic encryption (3DES) using a secret key. The main steps for the fPIN-creation of a person based on his NPR number are given in Fig.2.

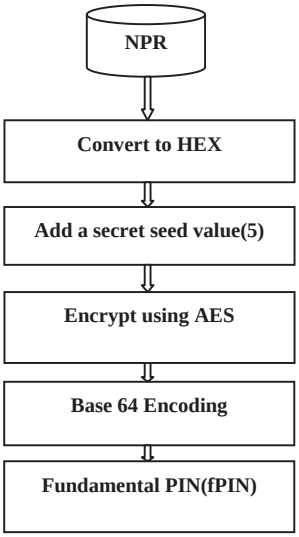


Fig.2 Derivation of fPIN

The Department Specific PIN [dsPIN)

In order to further protect the privacy, the derived fPIN would not be used for the identification purpose. Instead of using the fPIN in different governmental applications, several derivations of the fPIN, the so called Department Specific PIN (dsPIN) would be used. Each governmental department (i.e. different areas of the public administration) is assigned a specific alphanumeric code like Income Tax dept (IT), Health & Social Welfare Department (HS) etc.

For each of these departments, using the specific alphanumeric code, the proposed e-ID concept foresees a separate unique identifier, which is called the Department Specific PIN. The dsPIN is created by combining the fPIN with the sector specific alphanumerical code and then applying a cryptographic one way function, a Hash-function, to the result. Different dsPINs are thus generated for each governmental department based on the unique fPIN of a person. Each of these dsPIN is different and due to the application of one way function it is neither possible to calculate the underlying fPIN nor any other sector's dsPIN from a given dsPIN. In Fig.3 the basic steps of the dsPIN creation process are illustrated.

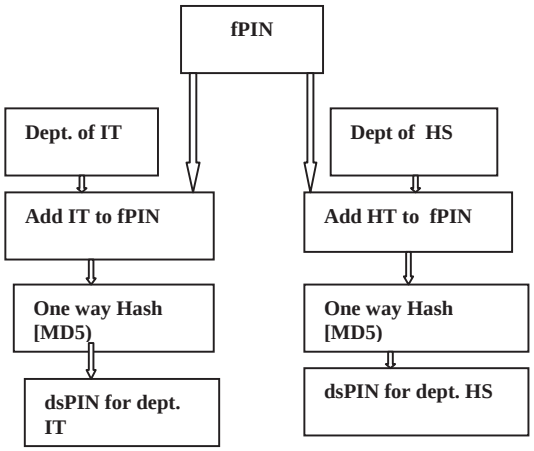


Fig 3 Department specific PIN

VI. THE SMART CITIZEN CARD CONCEPT

The Smart Citizen Card Concept is the proposed technological framework for the Indian e-ID concept. It would be used for the electronic identification and authentication of citizens. For authentication issues, the Citizen Card Concept would make use of digital signatures. Thus, the basis for a Citizen Card following this concept is a secure signature creation device. Such an implementation can be built up by the use of smart cards, but can also be realized using any other technical device which fulfils the requirements given in the concept, i.e. the requirements for the secure signature creation device.

For identification purposes the Citizen Card Concept makes use of the fPIN as defined before. In order to authenticate a citizen in relation to the fPIN, the concept of Linked ID is introduced. The Linked ID is a data structure that combines the fPIN of the citizen with the public key used for electronic signature. The Identity Linked ID is signed by the fundamental PIN Registration Authority to endorse its authenticity. By the use of the Identity Linked ID it is possible to create the relation between an electronic signature and the claimed identity. To do so the verifying application has to prove the electronic signature created by using the citizen card with the public key wrapped in the Linked ID. If the public key can be mapped to the electronic signature, the electronic signature can be considered as a proof of authenticity. In other words, it can be strongly assumed, that the person who possess the signature creation device (i.e. the citizen card) and knows the secret PIN to create signatures with it, is the person described in the Linked ID.

From the principle, an Identity Linked ID is similar to a digital certificate for electronic signatures. In contrast to a certificate, the Linked ID contains the fPIN which remains the same for a citizen throughout his lifetime, which cannot be guaranteed for the serial number of the digital certificate.

The linked ID would be one of the few places where the fPIN would be stored since the Linked ID itself would be under the sole control of the citizen. Storing the fPIN in the citizens' digital certificate for electronic signatures directly is not possible, since certificates have to be publicly available for signature verification purposes, but the fPIN has to be kept secure and secret.

VII. PROOF OF CONCEPT

For testing of our proposed solution the following hardware and softwares were used.

Hardware-Computer-Intel® core™ 2 Duo CPU,E7500@2.93GHz,2GBof RAM Physical Address Extension,500GB HDD

Operating System- Microsoft Windows XP Professional version 2002, SP2

Softwares Installed- Oracle VM VirtualBox on top which **Backtrack 5 R3** [a flavor of Linux used for Network Troubleshooting and Analysis) was installed

We used Forensics Hashing Tools menu of Backtrack and particularly used MD5 hashing algorithm.

We have used fictitious data of a person having the following attributes as in Table no.2. which are stored in the National Population Register

Table 2

Name	Amit Sharma
Date of Birth	12-12-1985
NPR number	A4562389654S
Aadhaar number	822111183521
PAN number	AAPNP7135L
Driving License number	RJ14/07/042/414254
Mobile Number	9325058244
E-mail address	amit@gmail.com

Example of our proposed solution -

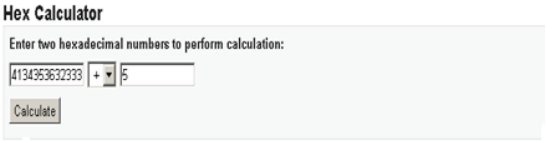
1. Convert the NPR number to its HEX value
   A4562389654S becomes **4134353632333839363553**[HEX)[13]

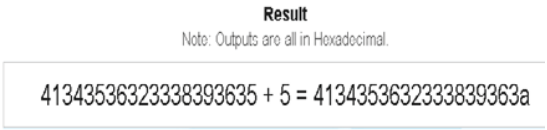
Here are the ASCII values of your

Char	Dec	Hex	Oct
A	65	41	101
4	52	34	64
5	53	35	65
6	54	36	66
2	50	32	62
3	51	33	63
8	56	38	70
9	57	39	71
6	54	36	66
5	53	35	65
4	52	34	64
S	83	53	123

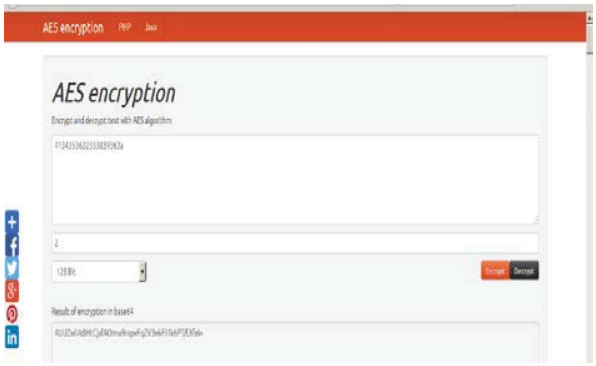
Copyright © 2014 ASCIIvalue.com

2. Add a seed value 5[HEX) to the above number [14]
   4134353632333839363553+5=
   413435363233383936355a[HEX)

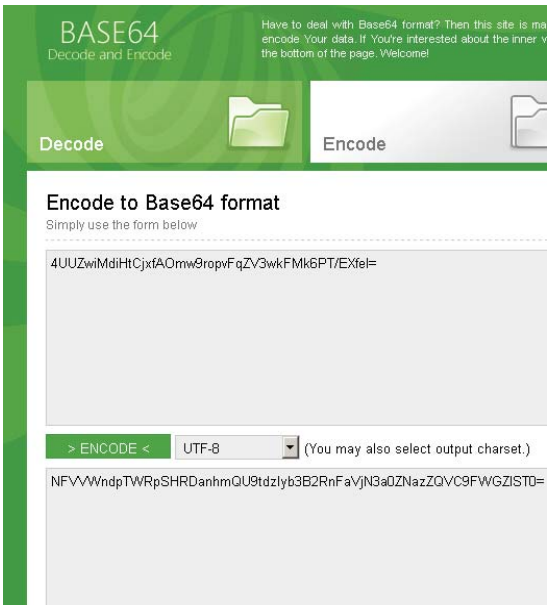




3. Encrypt the above value using AES, we get[15]
   4UUZwiMdiHtCjxfAOmw9ropvFqZV3wkFMk6PT/EXfeI=



4. Encode the value generated above by Base64 Encoding ,we get[16]
   NFVVWndpTWRpSHRDanhmQU9tdzlyb3B2RnFaVjN3a0ZNazZQVC9FWGZlST0=

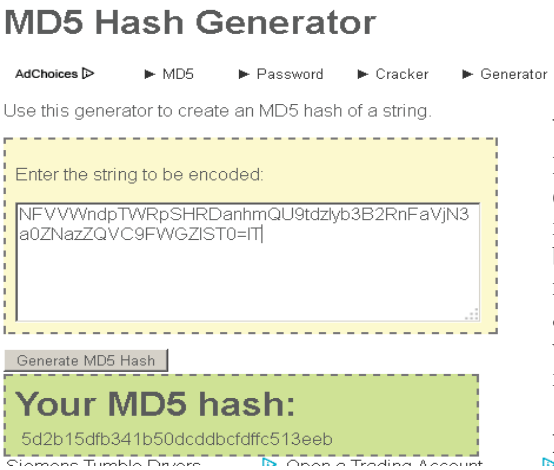


This will be the fPIN which will be stored in the smart ID card of the citizens.

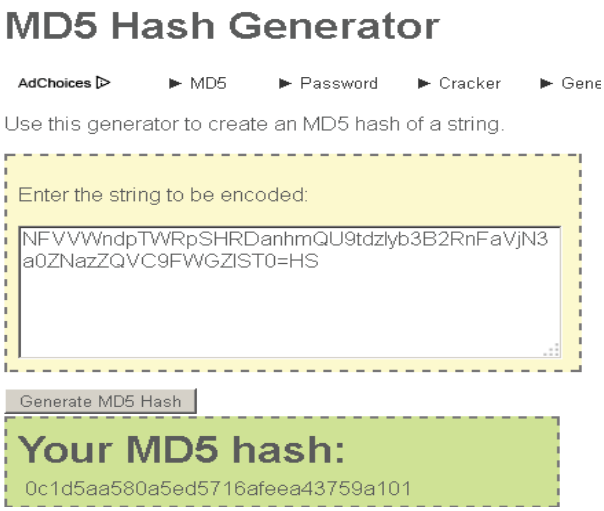
5. For deriving department specific PIN [dsPIN], add department ID say IT for Income Tax department **NFVVWndpTWRpSHRDanhmQU9tdzlyb3B2RnFaVjN3a0ZNazZQVC9FWGZlST0=IT**

   HS for department of Health & Social Welfare **NFVVWndpTWRpSHRDanhmQU9tdzlyb3B2RnFaVjN3a0ZNazZQVC9FWGZlST0=HS**

6. Apply one way Hash function [MD5] to the above concatenated values[17]
   Hence the dsPIN for IT department is **5d2b15dfb341b50dcddbcfdffc513eeb**



Hence the dsPIN for HS department is **0c1d5aa580a5ed5716afeea43759a101**



In our proposed solution all the citizens will be provided with smart citizen ID cards which will define the general requirements.

- **Secure electronic signatures**- i.e .legal equivalence to handwritten signatures
- **Additional key-pairs**-general signatures, encryption
- **Information Boxes to store Data**- Linked ID ,Certificates, ,Mandates/representation, Access control to Information box:

Hence the 'Citizen Card' is actually three electronic functions:

- The identification function
- The authentication function and
- The representation function

VIII. CONCLUSION

Making use of information technology does not necessarily endanger data protection. We have proposed a solution for identity management in e-government, which creates a balance between the risks arising from the application of new technology and the advantages offered by such application. It provides means of identification in the online world and at the same time preserves the privacy of the individual.

REFERENCES

[1]www.agimo.gov.au/infrastructure/authentication/agaf/glossary/i#identitymanagement.

[2]. A.Pandey, Dr. Jatinderkumar R. Saini. *An Analysis Of Online Identity Management Techniques* S.L. :

International Journal Of Research In Computer Application & Management, 2012, Vol. 2. Issn 2231-1009.

[3]. A.Pandey, Dr Jatinderkumar R. Saini. *Online Identity Management Techniques:Identification and Analysis of Flaws and Standard Methods* , s.l. : International Journal of Innovative Research & Development, 2012, Vol. 1. 2278 – 0211.

[4]. A.Pandey & Jatinderkumar R .Saini. *An Investigation of Challenges to Online Federated Identity Management* , s.l. : International Journal of Engineering Innovation & Research, 2013, Vol. 1. ISSN : 2277 – 5668.

[5] A. Pandey & Jatinderkumar R. Saini,*" Identity Management in E-Governance*" Volume 2, Issue 5, September – October 2013, *IJETTCS*, ISSN 2278-6856

[6] Kumaraguru, P., and Cranor, L. *Privacy in India: Attitudes and Awareness*. In Proceed-ings of the 2005 Workshop on Privacy Enhancing Technologies (PET2005) (30 May - 1 June 2005).

[7] http://www.krepcio.com. *http://www.krepcio.com/images/1agg-TIMELINE-7-SocNet.jpg.* [Online] krepkio.

[8]. Rouault, Jan De Clercq and Jason. *An Introduction to Identity Management. http://devresource.hp.com/.* [Online] http://devresource.hp.com/drc/resources/idmgt_intro/index.jsp#authors.

[9]. **IDC.** *Spending in India to grow at 16.3% to $43.57 bn in 2012:*. s.l. : IDC.

[10] Edgar Whitley And Gus Hosein ," *Global Challenges For Identity Policies"*, Palgrave Macmillan, 12th November 2009

[11] Eghbal Ghazizadeh et. al s.l. : IEEE , 2012. *"A Survey on Security Issues of Federated Identity on the Cloud."*

[12] *http://ditnpr.nic.in/FAQs.aspx.* [Online] Department of Information Technology,India, July 2014.

[13] http://asciivalue.com/

[14] http://easycalculation.com/hex-calculator.php

[15] http://aesencryption.net/

[16] http://www.base64decode.org/

[17] http://www.md5hashgenerator.com/

AUTHORS' PROFILE

Aparajita Pandey is an Assistant Professor at B.I.T.(MESRA),Jaipur Campus. Her qualifications include B.E.(EEE) ,MBA. She is also a MCSE and has a diploma in Cyber law. She has teaching experience of about 12 years in the areas of Circuit Analysis, Data Communication and Computer Networks. She is also a member of IAENG and ISOC. Her research interests include Online Identity Management, Internet Trust, Privacy and Network Security.

Dr. Jatinderkumar R. Saini is Ph.D. from Veer Narmad South Gujarat University, Surat, Gujarat, India. He secured first rank in all three years of MCA in college and has been awarded gold medals for this. He is also a recipient of silver medal for B.Sc. (Computer Science).
He is an IBM Certified Data Associate- DB2 as well as IBM certified Associate Developer- RAD. He has presented 14 papers in international and national conferences supported by agencies like IEEE, AICTE, IETE,ISTE, INNS etc. One of his papers has also won the 'Best Paper Award'.9 of his papers have been accepted for publication at international level and 13 papers have been accepted for national level publication. He is a chairman of many academic committees. He is also a member of numerous national and international professional bodies and scientific research academies and organizations.