International Journal of Security and Its Applications
Vol.8, No.1 (2014), pp.103-112
http://dx.doi.org/10.14257/ijsia.2014.8.1.10

Securing E-Governance Services through Biometrics

Madhavi Gudavalli[1], Dr. D. Srinivasa Kumar[2] and Dr. S. Viswanadha Raju[3]

*[1]Research Scholar of JNTU Hyderabad and Assistant Professor Department of IT
JNTUK University College of Engineering Vizianagaram,
Vizianagaram, Andhra Pradesh, INDIA
[2]Professor & Principal Department of CSE, Nalanda Institute of Engineering &
Technology, Guntur, Andhra Pradesh, INDIA
[3]Professor in CSE, School of Information Technology, Jawaharlal Nehru
Technological University (JNTUH), Kukatpally, Hyderabad INDIA
[1]madhavik4u@gmail.com, [2]srinivaskumar_d@yahoo.com,
[3]viswanadha_raju2004@yahoo.co.in*

Abstract

E-governance is the application of information & communication technologies to transform the efficiency, effectiveness, transparency and accountability of informational & transactional exchanges with in government, between government & government agencies of National, State, Municipal & Local levels, citizen & businesses, and to empower citizens through access & use of information. Pervasive services of virtual communities and digital governments are achievable only if trust, privacy and security can be secured and strengthened. To meet these requirements, mechanisms, which provide secure management of information and facilities without compromising privacy and civil rights, have to be devised. The success of such mechanisms relies on effective identity authentication. While traditional security measure such as PINs and passwords may be forgotten, stolen, or cracked, biometrics provides authentication mechanisms based on unique human physiological and behavioural characteristics that can be used to identify an individual or authenticate the claimed identity of an individual, but cannot be easily duplicated or forged. This paper discusses the role of biometric authentication in e-governance environment to provide services efficiently and securely over the internet.

Keywords: *Biometrics, E-Governance, Identity and Access Management, UIDAI*

1. Introduction

Governments are using the Internet and e-commerce technologies to provide public services to their citizens. In so doing, governments aim to form better relationships with businesses and citizens by providing more efficient and effective services. E-government provides opportunities to streamline and improve internal governmental processes, enable efficiencies in service delivery, and improve customer service. New technologies constantly evolve new dimensions to daily life. They can be used to provide interactions between users and their governments through electronic services. Governments are looking for more efficient and effective uses of technology in order to electronically deliver their services [1, 15]. Electronic government (e-government) has therefore become an important world-wide application area. With e-government applications, users are required to provide governments with personal information which necessitates an efficient, secure technology to provide reliable methods, particularly for users' identification as well as secure information systems.

ISSN: 1738-9976 IJSIA

Thus, the implementation of e-government is facing important issues such as information security, user authentication and privacy in which biometric authentication is a potential solution to deal with such concerns [12]. It can provide reliable identification of individuals as well as the ability for controlling and protecting the integrity of sensitive data stored in information systems [14]. As a result, several governments have implemented biometric authentication systems in order to efficiently and securely provide their services. However, the adoption of biometrics in e-government has become a major component of political planning for several governments. In particular, user acceptance can be an essential factor for the successful implementation of biometrics [6, 13, 15]. Moreover, users can have a direct impact on the operational performance of biometric systems, so their concerns need careful consideration, even if their concerns are fairly rough and ill defined [6].

2. Background

2.1. e-Governance

e-Governance is a technology-mediated relationship between citizens and their governments from the perspective of potential electronic deliberation over civic communication, over policy evolution and in democratic expressions of citizen will [2]. In developing countries access to the government service is not convenient and simple task. The services are citizenship records, police records, ration card application, agriculture services, hospital services, BPL services and pension scheme. There a long procedure of to get these services and it takes lots of time of citizen. The situation is same all over across the India. The main reason behind it is manual work. For complication of application it needs to be processed through many persons and departments. The new approach as the solution to all these problems is e-Governance (electronic governance), also known as e-government, online government, digital governance. E-Governance provides services, transactions and interactions with citizens, business and other arms of government with the use of information and communication technology.

Electronic government involves the citizens of that country in certain government activities in order to help solve problems. E-government provides unparalleled opportunities to streamline and improve internal governmental processes, enhance the interactions between users and government, and enable efficiencies in service delivery [15]. It refers to the use of information technology by government agencies in order to enhance the interaction and service delivery to citizens, businesses, and other government agencies [1, 4]. Thus, there are four categories of e-government applications which are: Government-to-Citizen (G2C); Government-to-Business (G2B); Government-to-Government (G2G); and Government-to-Employee (G2E) [4].

2.2. Digital and Cultural Gap

Digital divide refers to the gap between the group of people that are very familiar and have good access to high technology and those who do not [7]. It can be a result of several reasons such as a lack of financial resources, great education, and computer literacy. However, the digital divide makes the successful of e-government applications challenging [3]. A digital divide can be caused by the lack of knowledge and experience with technology, for instance, people in rural areas and inner city neighborhoods may have less internet access than others, while those who have never used computers may simply be reluctant to use the new technology [1].

2.3. Biometric Authentication Technology

Biometrics refers to automatic identity authentication of a person on a basis of one's unique physiological or behavioral characteristics [10]. A biometric system is a pattern recognition system that functions by acquiring biometric data from an individual, extracting a feature set and comparing this feature set against the template set stored in the database. Depending on context the biometric systems may function either in verification mode or identification mode.

In verification mode, the system authenticates a person's identity by comparing the obtained biometric data against biometric template(s) stored in the system database. Verification is positive recognition; where the aim is to avoid multiple people from using the same identity. While in identification mode, the system distinguishes an individual by searching the templates of all the users stored in the database for a match. Identification is negative recognition: prevent a single person from using multiple identities. While convention techniques of personal recognition such passwords, PINs, tokens and keys may work for positive recognition, negative can only be ascertained through biometrics. Figure 1 shows sample biometrics used either in verification mode or identification mode.

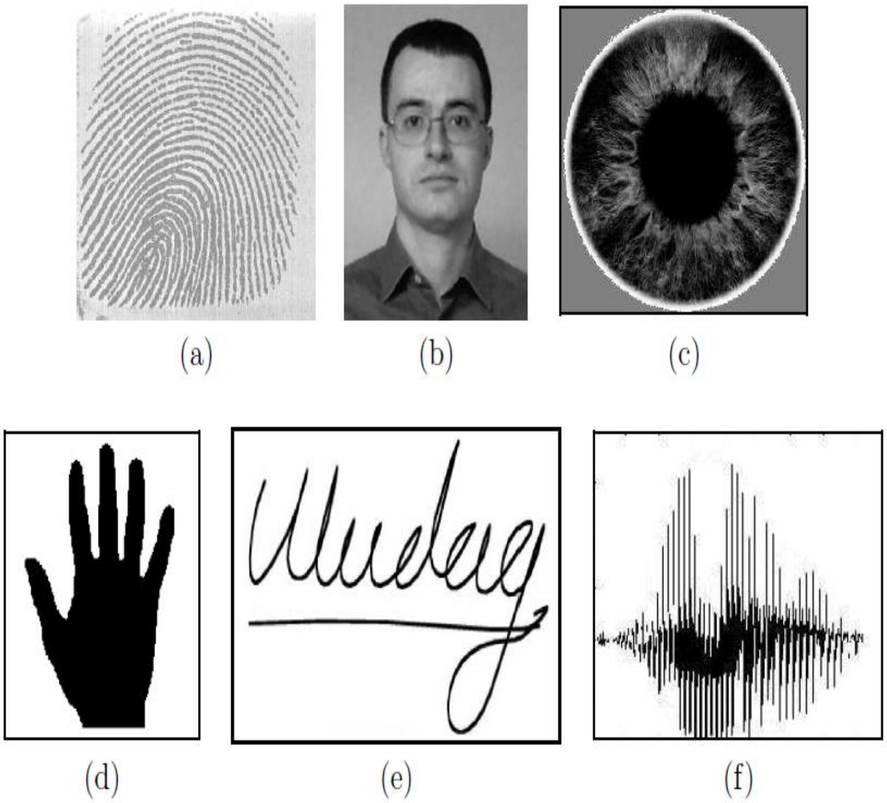

Figure 1. Sample Biometric Traits: (a) Fingerprint, (b) Face, (c) Iris, (d) Hand Geometry, (e) Signature, and (f) Voice

The strong database needed for a successful e-governance is vulnerable to fraud. There are attempts being made to come up with "Biometric" techniques, which are more secure. The password can be replaced as an individual's mark of identity. Similarly, password can be replaced by fingerprints or facial characteristics to verify the identity. Instead of having card readers, there should be devices like fingerprint readers or eye scanners. Common Biometrics implemented or studied includes fingerprint, face, iris, voice, and signature and hand geometry. It is one of the important evolving technologies, which will ensure the security and privacy issues as well. The market is full of such type of computers and laptops.

Biometric technology usually involves a scanning device and related software which can be used to gather information that has been recorded in digital form [8]. Having digitally collected the information, a database is used to store this information for comparison with the previous records. When converting the biometric input, namely the already collected data in digital form, this software can now be used to identify the specific inputs into a value that can be used to match any data previously collected. By using an algorithm, the data points are then processed into a value that can be compared with biometric data in the database [8].

2.4. Requirement of Biometric in e-Governance

Biometrics has been widely used in forensics, such criminal identification and jail security and has the possibility to be widely adopted in a very broad range of government services

1) Banking security, such as electronic fund transfers, ATM security, check cashing and credit card transactions;
2) Physical access control, such as airport access control;
3) Information system security, such as access to database via login privileges;
4) Government benefits distribution, such as welfare disbursement programs;
5) National-id systems, which provide a unique id to the citizens and integrate different government services;
6) Voter and driver registration, providing registration facilities for voters and drivers
7) Customs and immigration, such as the Immigration and Naturalization Service Passenger Accelerated. Service system (INSPASS) which permits faster immigration procedure based on hand geometry.

2.5. Examples of Biometric Technology in E-government Applications

By using biometric technology, e-government aims to give its citizens improved services with efficient and secure access to information by providing reliable identification of individuals as well as the ability for controlling and protecting the integrity of sensitive data stored in information systems. Currently biometric technology is used for applications like e-voting to ensure that voters do not vote twice. With biometric technology, governments are better able to prevent fraud during elections and other transaction types. Moreover, biometric technology has most recently been used to ensure correct working times are recorded and that only authorized personnel have access to government property and resources.

Biometric technology can also be used by e-governments for business. For instance, banks frequently adopt a facial feature recognition system to ensure that there is a reduced potential for theft. For example, photos are taken on the bank slips which are stored on computer software. As a result, this has avoided the issue of fraudulent bank slips when withdrawing money at ATMs. These technological advances in authenticating dealings with business have helped the government to conduct its activities more effectively and more securely [9].

In business transactions there is frequently the need for full authentication of employees to ensure that, in case of any problem, management is in a position to identify the person responsible for that act. Commercial applications may also require full identification capability, digital certificates, human interface, and one or more authentication devices to ensure that the business can run safely and effectively. People are also in a position to do their business with increased trust. Digital trust through public key cryptography, strong authentication and certification allows greater transaction confidence as long as that organization has a certified identity as an effective and trustworthy company [6].

Biometric technology is also used in the identification of citizens by e-government applications. Every nation could ethically be able to identify its citizens and differentiate non-citizens by using variations of national identification cards, visas, and passports with biometric data encoded within. Prior to the use of biometric data with such documents they were too easily forged or altered to allow unauthorized access to resources and facilities. As a result many nations have avoided the use of mechanisms such as a national identity card in the past. Effective e-government biometric applications to authenticate and identify citizens have effectively been used in reducing the issues of illegal immigration, access bottlenecks in busy facilities and high costs of employing security personnel.

3. The Basic Structure of e-governance

E-governance can be attained in four steps. Based on technical, organizational and managerial feasibilities, the four stages of a growth model for e-governance[5] are:

- Cataloguing (Information)
- Transaction
- Vertical integration (Interactive)
- Horizontal integration (Strategic, interactive) or transformation

These four stages are arranged in terms of complexity and different levels of integration. Figure 2 shows the stages of e-governance. The first stage is *"cataloguing" or "Information"* because efforts are focused on cataloguing government information and presenting it on the web. The first stage is focused on establishing an on-line presence for the government.

The second stage "*Transaction"*, where e-government initiatives are focused on connecting the internal government system to on-line interfaces and allows citizens to transact with government systems to on-line interfaces and electronically, is referred as "transaction-based" e-government. This stage is a link between the live database and the on-line transaction. However, the critical benefits of implementing e-governance are actually derived from the integration of underlying processes across different level of government. Any citizen can contact one point of government to complete any level of governmental transaction, which can be referred as "one stops shopping" concept. This integration may happen in two ways: vertical and horizontal.

Vertical integration refers to local and central administration connected for any functions or services of government, while *horizontal integration* refers integration across different functions and services. Vertical or intra- departmental integration is must before implementing the horizontal or interdepartmental integration because of different level of complexities associated. It is expected that vertical integration across different levels of government should happen first, because the gap between the levels of government is much less comparatively [5] than the difference between different functions. Mostly administrators interact more closely with their central or local counterparts than with other departments in the same level of government. The *vertically* and *horizontally* integrated e-government represents an ideal situation, in which citizens have on-line access to ubiquitous government services, with a transparent system.

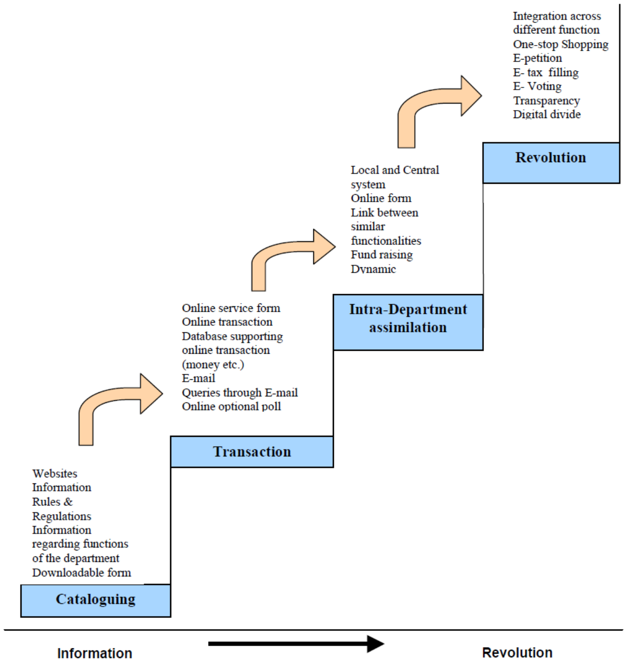

Figure 2. Stages of e-governance

4. Role of Biometric Technology in aadhaar Authentication i.e UIDAI Authentication

The Unique Identification Authority of India (UIDAI) has been created with the mandate of providing a Unique Identity (Aadhaar) to all residents of India. Aadhaar enrolment has picked up momentum with over 27,000 enrolment stations conducting 10 Lakh enrolments every day across the country. The CIDR processes these enrolments by de-duplicating them to ensure uniqueness and then issues Aadhaar numbers. One of the mandates given to UIDAI is to define usages and applicability of Aadhaar for delivery of various services. Towards Aadhaar-enabled delivery of services and applications, UIDAI provides online authentication using the resident's demographic and biometric information [11]. The Aadhaar number, which uniquely identifies a resident, will give individuals the means to clearly establish their identity to public and private agencies across the country for service delivery.

Enrolment Process: Aadhaar enrolment has 2 main parts. The enrolment frontend, which consists of enrolment stations deployed across the country where people enroll for an Aadhaar number. The process of enrolment involves the collection of 4 demographic fields: name, address, date-of-birth and gender and the capture of biometrics – which includes all 10 fingerprints, 2 irises and a photo of the face. This enrolment information is securely encrypted and sent to the CIDR. The Enrolment backend operations are carried out at the CIDR, where the packet is checked and validated for correctness and then de-duplicated against the existing enrolment database. Only when the new enrolment record is found to be unique is an Aadhaar number granted to that particular resident.

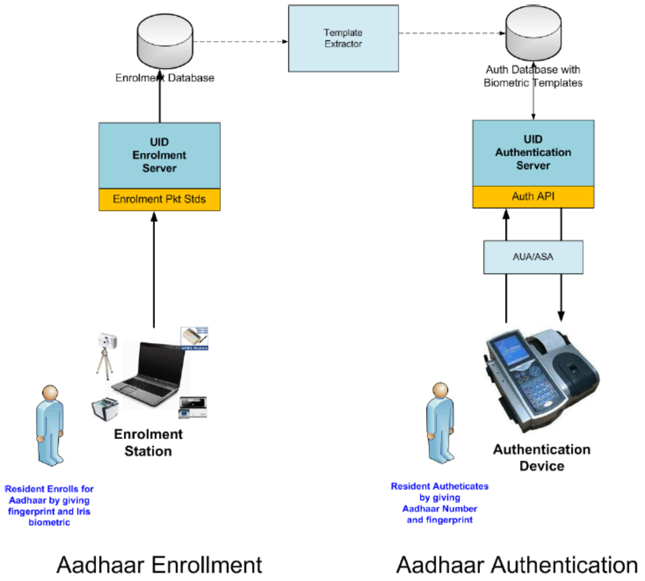
Template Extractor
Enrolment Database
Auth Database with Biometric Templates
UID Enrolment Server
Enrolment Pkt Stds
UID Authentication Server
Auth API
AUA/ASA
Enrolment Station
Authentication Device
Resident Enrolls for Aadhaar by giving fingerprint and Iris biometric
Resident Autheticates by giving Aadhaar Number and fingerprint
Aadhaar Enrollment
Aadhaar Authentication

Figure 3. Aadhaar Enrolment and Authentication

Aadhaar Authentication: Aadhaar Authentication is the process wherein, Aadhaar number along with the Aadhaar holder's personal identity data is submitted to the CIDR for matching, following which the CIDR verifies the correctness thereof on the basis of the match with the Aadhaar holder's identity information available with it. Since the Aadhaar number is mandatory during an authentication transaction, the appropriate resident's record can be fetched and a simple 1:1 match of the biometric/demographic data can complete the authentication transaction. To protect resident's privacy, Aadhaar Authentication service responds only with a "Yes/No" and no Personal Identity Information (PII) is returned as part of the response [11]. Aadhaar Authentication enables 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 can help agencies in delivering services to eligible beneficiaries based on establishing their identity, thus improving efficiency and transparency in service delivery to the common man.

5. Conclusions

Governments are concerned about user verification and system security in developing e-government services particularly with moves towards combined, seamless services, which are delivered electronically. As the levels of worldwide information system security breaches and transaction fraud increase, the imperative for highly secure authentication and personal verification technologies becomes increasingly pronounced. As a result the potential benefits of biometrics, in particular identification issues and security, are gaining importance on political agendas for e-government development.

The range of potential biometric technologies being considered for differing situations to support the provision of services has an important impact on the likely success of the implementation effort. The task force identified that each technology has particular strengths and weaknesses and as such no single technology is likely to suit all applications. The two variables that influence the implementation of biometrics in the public domain were identified as a) public perception of the technology, and b) performance of the technology. Fingerprint scanning was identified as being the most accurate technology, however it has the lowest public acceptance rate given the associations with criminality. The technology with the highest level of public acceptance is facial scanning, however this is the weakest performing technology, as there are difficulties in distinguishing between similar facial images. The technology that satisfies both public perception and performance criteria is iris scanning which does not require physical contact and is accurate.

Recognizing areas of vulnerability is key to good deployment of biometrics. Wide-scale deployments, such as India's UID scheme, which will provide a unique identification number to all 1.25 billion of its people, and the use of biometrics for mobiles and other consumer technology, have given biometrics a secure foothold in public and private industries worldwide. Biometrics also have cost benefits. Passwords, PINS and ID cards all have an ongoing cost, both with the physical replacement of lost ID cards and the administration of new cards and passwords. Biometrics simply require a one-off enrolment, after which only the eye/finger/face etc. must be presented to the biometric reader to enable access.

Acknowledgements

We would like to express our gratitude to all those who have helped directly or indirectly the possibility to completion of this paper. We also would like to thank referees authors of this paper. Finally we would like to say special thanks to the IJSIA journal for accepting this paper.

References

[1] S. Alharbi, “Perceptions of Faculty and Students toward the Obstacles of Implementing EGovernment in Educational Institutions in Saudi Arabia”, West Virginia University, **(2006)**.

[2] F. Bannister and R. Connolly, “New Problems for Old? Defining e-Governance”, proceedings of the 44th Hawaii International Conference on System Sciences, **(2011)**.

[3] A. Al-shehry, S. Rogerson, N. Fairweather and M. Prior, “The Motivations for Change towards E-government Adoption: Saudi Arabia as a case Study”, eGovernment Workshop. Brunel University, West London, **(2006)**.

[4] H. AlShihi, “Critical Factors in the Adoption and Diffusion of E-government Initiatives in Oman”, PhD thesis, Victoria University, Australia, **(2006)**.

[5] M. Shah, “E-Governance in India: Dream or reality?”, International Journal of Education and Development using Information and Communication Technology (IJEDICT), vol. 3, no. 2, **(2007)**, pp. 125-137.

[6] J. Ashbourn, “Practical biometric from aspiration to implementation”, London: Springer, **(2004)**.

[7] A. Blau, “Access isn't enough: Merely connecting people and computers won't close the digital divide”, American Libraries, vol. 33, no. 6, **(2002)**, pp. 50-52.

[8] R. Bolle, J. Connell, S. Pankanti, N. Ratha and A. Senior, “Guide to Biometrics. New York: Springer, **(2004)**.

[9] K. Bonsor and R. Johnson, “How Facial Recognition Systems Work, How Stuff Works”, viewed on 1st October 2007 at http://computer.howstuffworks.com/facialrecognition.htm.

[10] W.-S. Chen, K.-H. Chih, S.-W. Shih and C.-M. Hsieh, “Personal Identification Technique based on Human Iris Recognition with Wavelet Transform”, 2005 IEEE, ICASSP, **(2005)**, pp. II -949.

[11] “Role of Biometric Technology in Aadhaar Authentication”, UIDAI, **(2009-2012)**.

[12] B. Dearstyne, “E-business, e-government and information proficiency”, Information Management Journal, vol. 34, no. 4, **(2001)**.

[13] I. Giesing, “User response to biometric”, University of Pretoria, 14 Thamer Alhussain and Steve Drew, **(2003)**, pp. 95-135.

[14] B. McLindin, “Improving the Performance of Two Dimensional Facial Recognition Systems”, University of South Australia, **(2005)**.

[15] M. Scott, “An assessment of biometric identities as a standard for e-government services”, Services and Standards, vol. 1, no. 3, **(2005)**, pp. 271-286.

Authors

Madhavi Gudavalli received the B.Tech(CSIT) from JNTU , M.Tech(CSE) from JNTU Hyderabad and registered Ph.D in Computer Science & Engineering discipline from JNTU Hyderabad in 2011. She is currently working as Assistant Professor in the Department of Information Technology at **JNTUK University College Of Engineering Vizianagaram**. She guided many projects in the area of image processing for CSE & IT Departments. Her research interests are in the areas of Biometrics and Image Processing. Her research articles are accepted in international Conferences and journals and proceedings are published in IEEE, ACM digital libraries. She played a vital role in AICTE-NBA Accreditation work at CVR college of Engineering, Hyderabad in 2007. She conducted several workshops/seminars/conferences at institutional level. She was sanctioned with Major Research Project entitled **A Next Generation Identity Verification System To Provide Security** in the area of Biometrics as Co-Principal Investigator by **AICTE** under Research Promotion Scheme. In recognition of her outstanding scientific contributions her research articles received Travel grant from **DST** and **UGC**. She is one of the inventors of the **THREE Patents** filed in the area of Biometrics, Vehicular Automation and Cloud Computing. She is a Life member in different Professional bodies such as ISTE and CSI. Her research contributions are not only confined to subject area but also extended to other related domains arising out of the new education system, assessment and accreditation, and their impact on Indian Higher Education. As an off shot of research endeavour's her papers were accepted and presented in **World Education Summit (WES 2012-AICTE)** entitled *International Practices In Assessment, Accreditation & Quality Standards In Higher Education*. The hallmarks of her illustrious career include teaching Engineering and Technology and pursuing exemplary research on improving security by using advanced tools of Biometric systems.

Dr. Srinivasa Kumar Devireddy received the B.E. degree in Computer Science & Engineering from Karnataka University, Dharwad in 1992, M.S. degree in Software Systems from Birla Institute of Technology and Science, Pilani in 1995 and Ph.D. in CSE from JNTU Hyderabad in 2010. He is currently working as Professor in the department of Computer Science & Engineering and Principal at Nalanda Institute of Engineering & Technology, Guntur. He is a senior member of IEEE. He guided many projects in the areas of image processing, Biometrics and content based Image Retrieval. His research articles are accepted in international Conferences and journals and proceedings are published in IEEE, ACM digital libraries.

Dr. S.Viswanadha Raju working as Professor of Computer Science and Engineering Department at SIT, JNTUniversity Hyderabad. He is a distinguished academician whose advanced research work in the field of Programming in C, Information Retrieval, Data Mining, Biometric Systems and Research Methodology are globally recognized. He filed **THREE patents** deriving from his research and also received awards from various bodies on the basis of his contribution. Dr.S.V.Raju was sanctioned with two Major Research Projects by AICTE under Research Promotion Scheme. He has been granted funds from national organizations such as Dept. of Science and Technology (DST), AICTE, UGC etc to encourage research on his domains. He has given several invited talks and tutorials in Research Methodology, Programming tips, Algorithms, Information Retrieval, Data mining, Biometrics and relevant areas. He visited Singapore and Taiwan to attend international conference for presenting research work and he received Travel grant from UGC. He is the life member of IETE, ISTE, CSI and IACSIT. He guiding or guided more than 42 students/scholars: Ph.D., (12) and M.Tech/MCA (29) besides guiding a large number of student projects. He is credited with 50 research publications in National and International journals repute. His research contributions are not only confined to his subject area but also extend to other related domains arising out of the new education system, assessment and accreditation, and their impact on Indian Higher Education. To add impetus to his academic credentials he has undergone training for the quality improvement in education at NITTTR, WOSA-2012, TCS, Infosys, and NBA etc. He conducted an International Conference on Advanced Computing Technologies 2008 with the capacity of Convener. He served as Head of dept of CSE at JNTUHCEJ and also as Director of MCA (Accredited by NBA) and proceeding to this served as a Head of the Dept of CSE/MCA (CSE-Twice accredited by NBA) at GRIET. He initiated and actively participated in AICTE approval, accreditation (NBA) , NAAC and TEQIP work etc. he played a instrumental roles in organizing various conferences, seminars, workshops and acted as convener, coordinator etc.