



ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Implementation of Empowered E-Governance Using Secured Cloud

A.Sangeetha¹ Dr.M.Deepamalar²

M.Phil Scholar, Post Graduate and Research Department of Computer Science, Parvathy's Arts and Science College,
Dindigul, India¹

Asst Professor, Post Graduate and Research Department of Computer Science, Parvathy's Arts and Science College,
Dindigul, India²

ABSTRACT: E-Governance has changed the way the users interact with the government. Information and Communication Technologies(ICT) has been a key contributor in the growth and success of e- governance. The magnified use of ICT has become a primary need for every individual to access the e-governance applications and to interact with in the entire Government framework. Through the e-governance, the government services will be made available to the citizen in a convenient, efficient and transparent manners. The cloud computing is a new way of computing which aims to provide better communication style and storage resources in a safe environment via the internet platform. The E-Governments around world are facing the continued budget challenges increasing in the size of their computational data and high level security for the citizens personal and transactional data so that they need to find ways to deliver their services to citizens as economically as possible without compromising the achievement of desired outcomes. The adoption of cloud computing with biometric security strategy for implementing E-Government architecture to improve E-Government efficiency of e-governance through cloud and also the use of biometric to overcome transparency and security aspects in order to function e-governance successfully.

KEYWORDS: G-Cloud, E-Governance, Biometric security.

I. INTRODUCTION

In today's world e-governance and Information and Communication Technologies (ICT) have bring together. ICT has revolutionized the way e-governance is being used now. Government is now delivering e-services which is proving a boon for the people. In moving towards digital India. With the usage of ICT, need for infrastructure and also storing of data of such a huge amount has become an area of concern. The cloud computing is a new way of computing which aims to provide better communication style, storage, computing power and ICT. Main goal of the cloud computing is to provide scalable and inexpensive on-demand computing infrastructures with good quality of service levels. Many companies developing and offering cloud computing products and services but have not properly considered the implications of processing, storing and accessing data in a shared and virtualized environment. In fact, many developers of cloud-based applications struggle to include security. In other cases, developers simply cannot provide real security with currently affordable technological capabilities. Cloud computing is sharing of resources on a larger scale which is cost effective and location independent. Resources on the cloud can be used by the client and deployed by the vendor such as amazon, google, IBM, salesforce, zoho, rackspace, Microsoft.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

II. ROLE OF CLOUD COMPUTING IN E-GOVERNANCE

A. E-GOVERNANCE

E-Governance is generally understood as the use of Information and Communication Technology (ICT) at all the level of the Government in order to provide services to the citizens, interaction with business enterprises and communication and exchange of information between different agencies of the Government in a speedy, convenient efficient and transparent manner.

E-Governance facilitates interaction between different stake holders in governance. These interactions may be described as follows:

- G2G (Government to Government)
- G2C (Government to Citizens)
- G2B (Government to Business)
- G2E (Government to Employees)

A.1 G2C (Government to Citizens)

E-Governance to Citizens in two-way communication allows citizens to instant message directly with public administrators, and cast remote electronic votes (electronic voting) and instant opinion voting. Transactions such as payment of services, such as city utilities, can be completed online or over the phone. Mundane services such as name or address changes, applying for services or grants, or transferring existing services are more convenient and no longer have to be completed face to face.

A.2 G2E (Government to Employees)

E-Governance to Employee partnership (G2E) is one of four main primary interactions in the delivery model of E-Governance. It is the relationship between online tools, sources, and articles that help employees maintain communication with the government and their own companies. E-Governance relationship with Employees allows new learning technology in one simple place as the computer. Documents can now be stored and shared with other colleagues online.

A.3 G2G (Government to Government)

E-government brings many advantages into play such as facilitating information delivery, application process/renewal between both business and private citizen, and participation with constituency. There are both internal and external advantages to the emergence of IT in government, though not all municipalities are alike in size and participation.

A.4 G2B (Government to Business)

Government-to-Business (G2B) is the online non-commercial interaction between local and central government and the commercial business sector with the purpose of providing businesses information and advice on e-business 'best practices'.

- G2B:Refers to the conduction through the Internet between government agencies and trading companies.
- B2G:Professional transactions between the company and the district, city, or federal regulatory agencies.
- B2G usually include recommendations to complete the measurement and evaluation of books and contracts.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

B. CLOUD COMPUTING

Cloud computing is a general term for the delivery of hosted services over the internet. Cloud computing enables companies to consume a compute resource, such as a virtual machine (VMs), storage or an application, as a utility just like electricity rather than having to build and maintain computing infrastructures in house. Although cloud computing has changed over time, it has been divided into three broad service categories: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

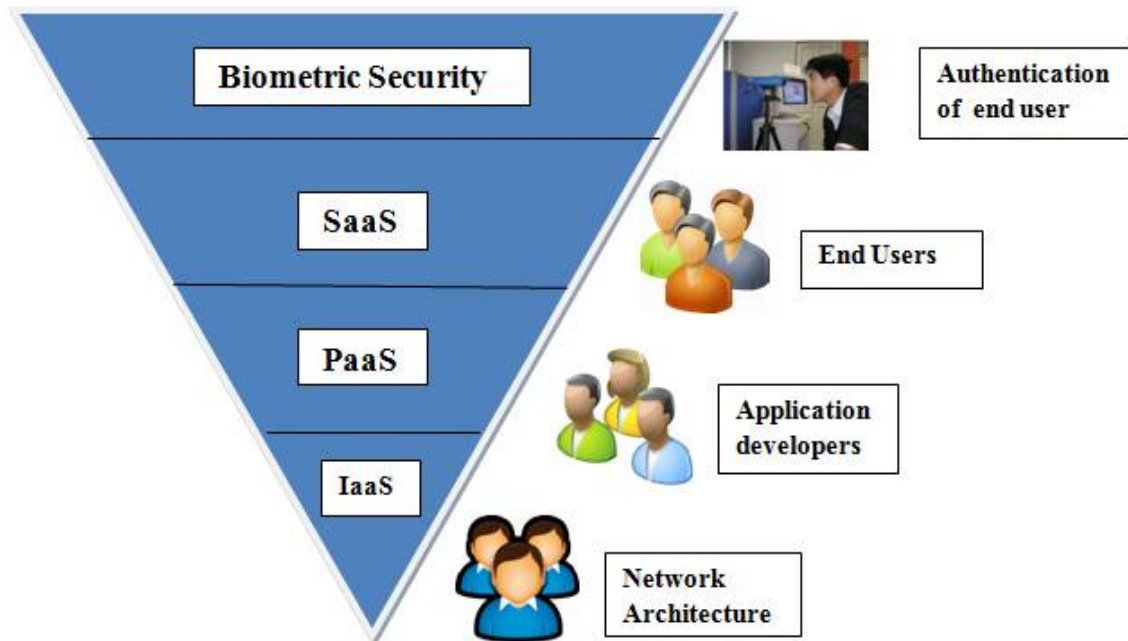


Figure1: Biometric security on value visibility to end-user

- **IaaS** providers, such as AWS, supply a virtual server instance and storage, as well as application program interfaces (APIs) that let users migrate workloads to a virtual machine. Users have an allocated storage capacity and can start, stop, access and configure the VM and storage as desired. IaaS providers offer small, medium, large, extra-large and memory- or compute-optimized instances, in addition to customized instances, for various workload needs.
- **PaaS** model, providers host development tools on their infrastructures. Users access these tools over the internet using APIs, web portals or gateway software. PaaS is used for general software development, and many PaaS providers will host the software after it's developed. Common PaaS providers include Salesforce.com's Force.com, AWS Elastic Beanstalk and Google App Engine.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

- **SaaS** is a distribution model that delivers software applications over the internet; these applications are often called web services. Microsoft Office 365 is a SaaS offering for productivity software and email services. Users can access SaaS applications and services from any location using a computer or mobile device that has internet access.

C. BIOMETRIC SECURITY

Biometric security is a security mechanism used to authenticate and provide access to a facility or system based on the automatic and instant verification of an individual's physical characteristics. Because biometric security evaluates an individual's bodily elements or biological data, it is the strongest and most foolproof physical security technique used for identity verification. Biometric security is mainly implemented in environments with critical physical security requirements or that are highly prone to identity theft. Biometric security-based systems or engines store human body characteristics that do not change over an individual's lifetime. These include fingerprints, eye texture, voice, hand patterns and facial recognition. An individual's body characteristics are pre-stored in a biometric security system or scanner, which may be accessed by authorized personnel. When an individual walks into a facility or tries to gain access to a system, the biometric scanner evaluates his/her physical characteristics, which are matched with stored records. If a match is located, the individual is granted access.

III. SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing and storage provides users with capabilities to store and process their data in third-party data centers. Organizations use the cloud in a variety of different service models (with acronyms such as SaaS, PaaS, and IaaS) and deployment models (private, public, hybrid and community). Security concerns associated with cloud computing fall into two broad categories: security issues faced by cloud providers (organizations providing software-, platform- or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud). The responsibility is shared, however. The provider must ensure that their infrastructure is secure and that their clients' data and applications are protected, while the user must take measures to fortify their application and use strong passwords and authentication measures.

IV. PROPOSED E-GOVERNANCE ARCHITECTURE ON SECURED CLOUD COMPUTING

Cloud computing has a lot of security issues that are gaining great attention nowadays, including the data protection, network security, virtualization security, application integrity, and identity management. Cloud computing and storage solution provide users and enterprises with various capabilities to store and process their data in third-party data centers by using the biometric security.

1. **User**– The different users are the stakeholders like citizens, business, employees and other government departments used service for different purposes. Users can download the difference documents and can fill online forms like passport, birth certificate etc. Also, they can make online payments for watertax, electricity, etc.
2. **Network** – Each of the users use their own network be it LAN or WAN to connect to the Internet so as to use the e-governance applications available on the cloud.
3. **Cloud Model**- Cloud Computing has evolved as a key computing platform for sharing resources that include infrastructures, software, applications, and business processes. e-governance plays a vital role in any organization and clouds with different layers are helpful to the e-Governance services.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

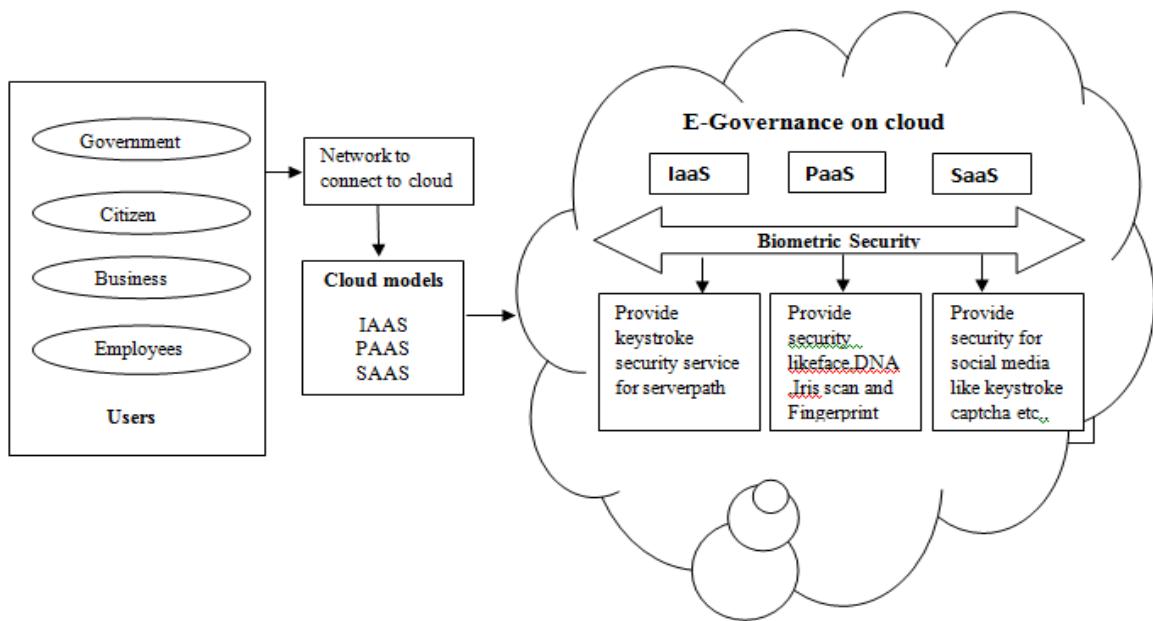


Figure2: Proposed e-governance Architecture on secured cloud computing

4. **E-Governance on Biometric secured cloud** – Here the dataset is stored and retrieved from. Whenever a data is on cloud, anyone from anywhere anytime can access data from the cloud since data may be common, private and sensitive data in a cloud.
5. **Biometric Security**– Here the Biometric security provide on three types of cloud computing service models IaaS, PaaS, SaaS. Sensitive data in a cloud computing environment emerge as major issues with regard to security in a cloud based system. Biometrics is the science and technology of measuring and statistically analyzing biological data for user authentication. Physical and logical access control applications using biometrics for the prevention of unauthorized access are expected to fuel the growth of this industry, bringing convenience with security.

D. MODEL CONSTRUCTION

E-Government application have the capability to transform the nation into an information society. The information of E-Government application need high level security to prevent fraudulent operations on citizen's personal and other sensitive information of government cloud helps enabling E-Government services faster and cheaper there by accelerating the adaptation and use of information technology for e-services. This proposed secured G-cloud architecture also provides biometric security for the e-governance application. The use of iris for identification is more robust as compared to others, so the iris biometric can be used for the verification of the authorized user in the e-governance cloud.

This biometric secured G-cloud is implemented by java. Iris recognition is implemented in cloud environment to recognize the authorized users of e-government applications. The proposed java application designed using the principle of biometric security architecture and deployed in cloud architecture will benefit the government in reducing

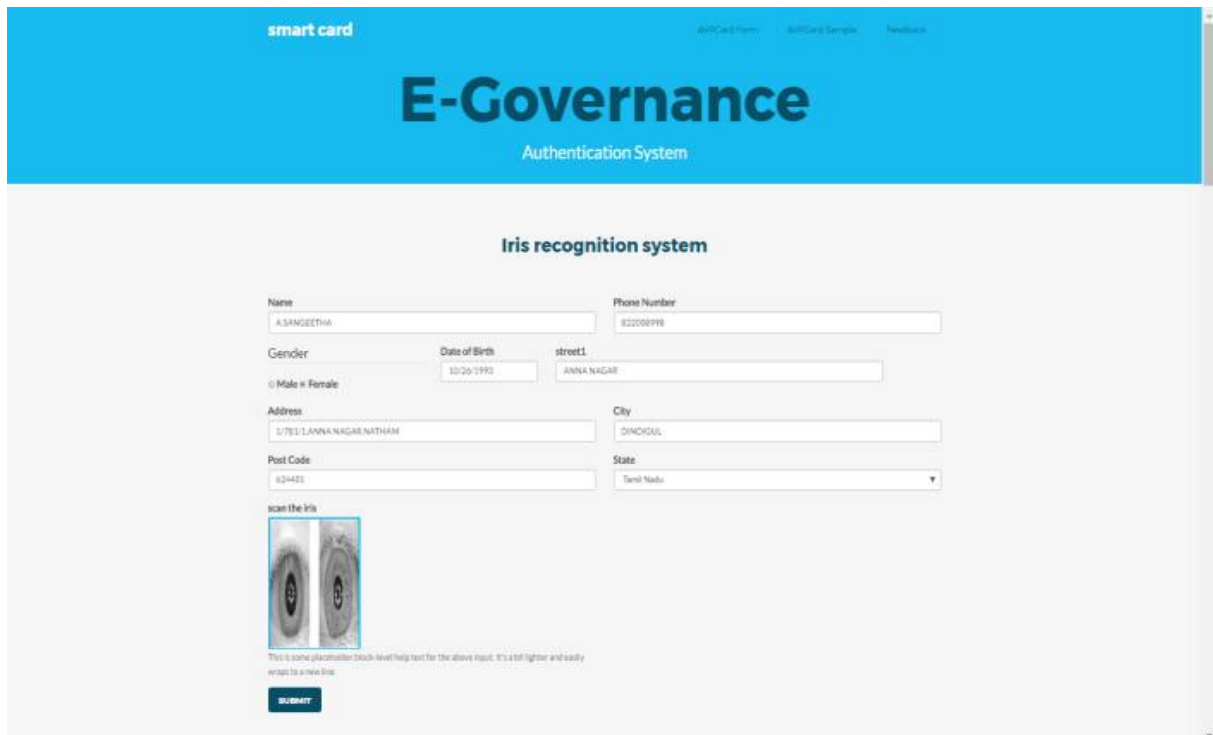
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

cyber crime on E-government and increasing the security on governance Figure 3 shows the API (Application Programming Interface) developed for biometric security on cloud, which is based on iris recognition.



The screenshot displays a web interface for an "E-Governance Authentication System". The main heading is "E-Governance Authentication System". Below this, there is a section titled "Iris recognition system". The form includes several input fields: "Name" (A.SANGEETHA), "Phone Number" (822008778), "Gender" (radio buttons for Male and Female), "Date of Birth" (10/20/1990), "street1" (ANNA NAGAR), "Address" (5/781/LANNA NAGAR,NATHAM), "City" (DINDIGUL), "Post Code" (624401), and "State" (Tamil Nadu). There is also a "scan the iris" section with two circular images of an iris scanner and a "Submit" button. A small note below the images reads: "This is some placeholder block-level help text for the above input. It's a bit lighter and easily wraps to a new line."

Figure3: Iris recognition system

To improve the security on E-government, the government should promote a smartcard as a single system for all smart-card applications. A single smart card started as identify cards carried by all citizens. The E-government application man include identify, travel documents, driver license, health information, an electronic wallet, ATM bank-card, public toll-road, Aadhaar, PAN card, house hold card and transit payments. Governments and regional authorities save money because of improved security, better data and reduced processing costs. These savings help reduce public budgets or enhance public services. Figure 4 proposed a single smart card model for multiple E-governance application.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

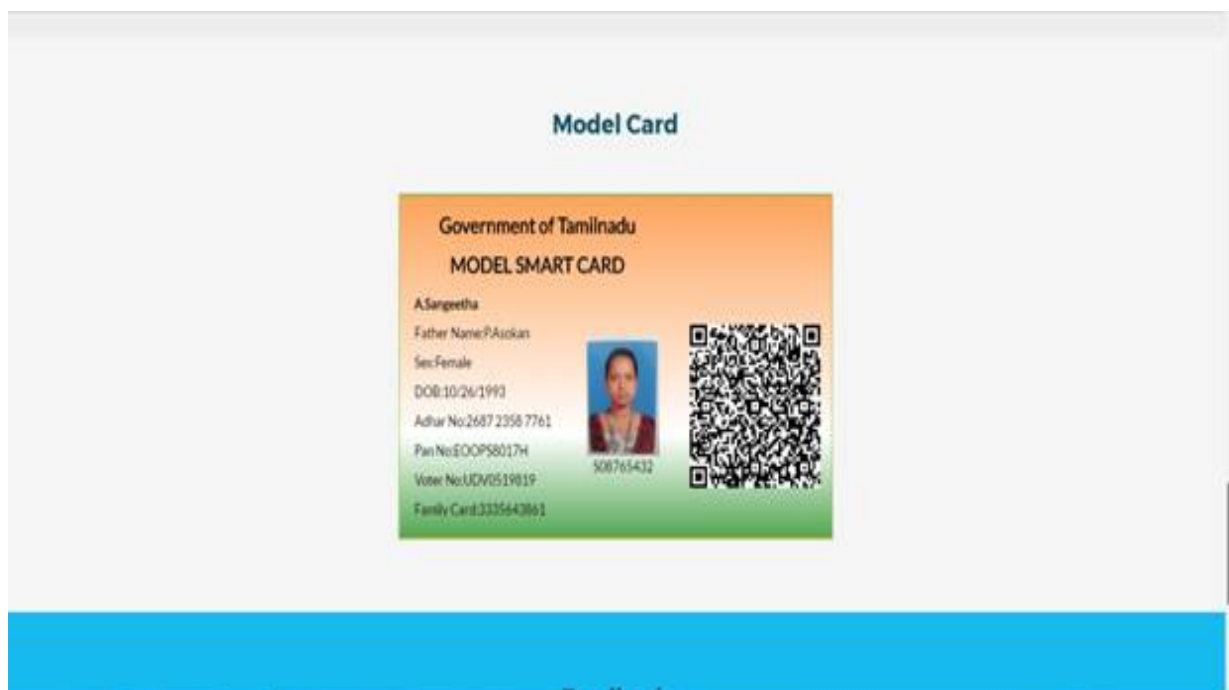


Figure4: Model Smart card

In this model construction API for biometric security on G-cloud is implemented using Java, but the smart card for multiple E-Governance application is a theoretical model which may be implemented in future

IV. RESULT AND DISCUSSION

BIOMETRIC IDENTIFICATION, or biometrics, refers to the process of identifying an individual based on his or her distinguishing characteristics. It comprises methods for uniquely recognizing humans based on one or more intrinsic physical and behavioral traits. The use of iris for identification is more robust as compared to others from the table so the iris biometric can be used for the verification of the authorized user on the e-governance cloud.

Biometric	Identify versus Verify	Robust	Distinctive
Fingerprint	Either	Moderate	High
Hand/Finger Geometry	Verify	Moderate	Low
Facial recognition	Either	Moderate	Moderate
Voice recognition	Verify	Moderate	Low
Iris scan	Either	High	High
Retinal scan	Either	High	High
Dynamic signature verification	Verify	Low	Moderate
Keystroke dynamics	Verify	Low	Low

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

E-governance has been boosted with the use of cloud and the biometrics. The challenges or the security issues with the implementation of cloud based e-governance are also resolved using biometrics also the iris is the best solution for the security as its more robust as compared to others after using the proposed scheme of e-governance all the required characteristics of its can be easily achieved.

V. CONCLUSION

Cloud computing is actually working to help break down the barriers of many government activities to enter new phase of collaboration and partnering, sharing services and pooling of resources. Cloud computing for e-governance offers an effective way to share information between citizens, reducing efforts in providing services, budgets management and cost effective. The challenges which the government has to deal with the security of the data on the cloud can overcome by providing fingerprint and Iris based biometric security on cloud. This proposed e-governance with biometric secured cloud offers transparent and secured services to the consumer, business, government. Government can use this proposed cloud e-governance with biometric security to protect that e-governance client and to secure the data from unauthorized users. This proposed secured e-governance cloud helps the user of the e-governance to maintain reliability and transparency on rendering e-governance services.

REFERENCES

- [1] Dr.NidhiSrivastava,"Effective e-governance through cloud computing",March 2016.
- [2] Tamara Almarabeh, Yousef Kh.Majdalawi, Hiba Mohammad,"Cloud computing of E-Government", Communication and Network,2016.
- [3] IIIT Hyderabad,"Cloud Computing for E-Governance - A white paper", January 2010.
- [4] Mahesh S.Darak, Dr. V.P.Pawar"Empowering E-Governance through Clouds & Biometrics", May-2014.
- [5] Rabi Prasad Padhy, ManasRanjanPatra , Suresh Chandra Satapathy, —"Cloud Computing: SecurityIssues and Research Challenges , International Journal of ComputerScience and Information Technology & Security" (IJCITS) Vol. 1, No. 2, December 2011.
- [6] Prince Jain, —"Security Issues and their Solution in Cloud Computing!", International Journal of Computing & Business Research, Proceedings of 'I-Society 2012' at GKU.
- [7]Wentao Liu. "Research on Cloud Computing Security Problem and Strategy", in: 2ndInternational Conference on Consumer Electronics, Communications and Networks (CECNet),April 2012.p.1216-1219.
- [8]Yuan, —"Cloud Computing and SecurityChallenges", 2012 ACM Publication.
- [9] MadhaviGudavalli, Dr. D. srinivasa Kumar2 and Dr. S.Viswanadha Raju, "Securing E-Governance services through Biometrics", International Journal of security and Its Applications.
- [10] KresimirPopovic and ZeljkoHocenski. "Cloud computing security issues and challenges", in:MIPRO,2010 Proceedings of the 33rd International Convention, 2010.p.344-349.