

Empowering E-Governance through Cloud & Biometrics

Mahesh S. Darak

Research Scholar

Dr. V.P. Pawar

Associate Professor

Abstract— The amplified use of ICT has become a primary need for every individual. E-Governance is the application of Information and Communication Technology (ICT) for delivering Government Services, exchange of information, communication transactions, integration various stand-alone systems and services between Government and Citizens (G2C), Government and Business (G2B) as well as back office processes and interactions within the entire Government frame work. Through the e-Governance, the Government services will be made available to the citizens in a convenient, efficient and transparent manner. The Combination of Cloud and E-governance collective can be productive to provide citizens good & transparent services. In this paper, we would see the increased efficiency of e-governance through cloud and also the use of biometrics to overcome transparency & security aspects in order to function e-governance successfully.

Index Terms— e-Governance, Cloud Computing, Biometrics, ICT, G2C, G2E, G2G, G2B, Security.

1 INTRODUCTION

The use of internet and other ICT Components had helped the government to provide citizens and organisations with more convenient access to the governments services and information. In late 1990s the first website came into existence of government was known as e-government. E-governance is a technological relationship between citizens and their government.

The traditional approach of accessing data in e-governance is very hard and not transparent as a one has to go many tables follow different rules and procedures for getting the relevant information. The e-governance has different users such as citizens, government, and businesses. The proposed scheme of using cloud and its security through biometric will make the working method and the data more transparent which the traditional system is lacking.

E-Governance is the public sector's use of information and communication technologies with the aim of improving information and service delivery, encouraging citizen participation in the decision-making process and making government more accountable, transparent and effective. E-Governance involves new styles of leadership, new ways of debating and deciding policy and investment, new ways of accessing education, new ways of listening to citizens and new ways of organizing and delivering information and services".

Cloud computing is the future generation computing, which provides storage, computing power, Information and Communication Technology (ICT) as a service for internet-based computing at nominal initial investment. Consumers can concentrate on their quality of service, without worrying about service-oriented problems. E-government provides opportunities to streamline and improve internal governmental processes, enable efficiencies in service delivery, and improve customer service. 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.

Cloud based E-governance represents an emerging paradigm for distributed computing of E-governance

applications that utilizes services as fundamental elements in building agile networks of collaborating applications distributed within and across government boundaries. In such open distributed computing environments, security is of paramount concern.

2.1 E-Governance

Electronic Governance has emerged as one of the flagship applications with aspiration to employ multimedia and network technologies to re-invent the way the government works. This IT enabled government will ensure better transparency and services to the public. India has since the last decade made rapid strides in the area of Information and Communication Technology. The objective of achieving Electronic Governance (EG) goes far beyond mere computerization of stand alone back office operations. It means to fundamentally change as to how the Government operates and this implies a new set of responsibilities for the executive, legislature and the citizenry. The effort should aim to bring about a social catharsis, which needs to be orchestrated in a comprehensive, concerted and planned fashion.

E-Governance is a process of reform in the way and delivers services to external and internal clients for the benefit of both government and the clients that they serve. Governments have innumerable applications that can be automated. Government spending increase the productivity of the government etc. Applications in the e-government.



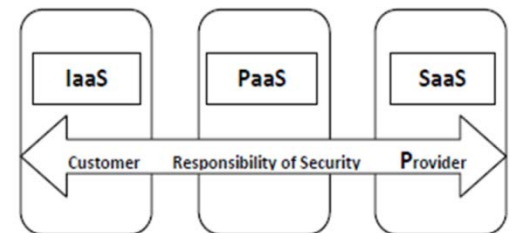
IT infrastructure is being setup and the way resources are being accessed.

The three cloud delivery models are:

Cloud Software as a Service (SaaS): Cloud consumers use software applications, but do not control the operating system, hardware or network infrastructure on which they are running.

Cloud Platform as a Service (PaaS): Cloud consumers use the platform upon which applications can be developed and executed.

Cloud Infrastructure as a Service (IaaS): Cloud consumers use basic computing resources such as processing power, storage, networking components or middleware on demand.



2.2 Cloud Computing

Cloud computing is the next natural step in the evolution of on-demand information technology services and products. The Cloud is a metaphor for the Internet, based on how it is depicted in computer network diagrams, and is an abstraction for the complex infrastructure it conceals. It is a style of computing in which IT-related capabilities are provided —as a service, allowing users to access technology-enabled services from the Internet (i.e., the Cloud) without knowledge of, expertise with, or control over the technology infrastructure that supports them. The technical foundations of Cloud Computing include Service-Oriented Architecture (SOA) and Virtualizations of hardware and software. The goal of Cloud Computing is to share resources among the cloud service consumers, cloud partners, and cloud vendors in the cloud value chain.

Cloud computing is a new business paradigm in a service oriented model, delivering business applications and other IT resources as services over the internet. It is a conglomeration

of infrastructure (hardware devices) and application software providing services to consumers on a pay-per-use basis. Cloud

computing represents the next generation infrastructure and application hosting service and delivery model. A cloud typically has three key differentiating characteristics: (a) the usage of the resources is on demand and billed at actual consumption, (b) is scalable and can support varying bursts of traffic, and more importantly, (c) can be accessed over the internet. Cloud represents a drastic variation from traditional infrastructure hosting that is done in a datacenter within the customer premises. Table 1 provides the key differences between traditional and cloud model from an ownership and service delivery perspective. Cloud computing comes in various types. Public, private and hybrid clouds define the manner and location in which the

Figure : Cloud Architecture

Four cloud deployment models are: Private or internal cloud, community cloud, public cloud and hybrid cloud.

Private: Private Cloud is operated only for particular organization. It may be managed by the particular organization itself or third party cloud providers.

Community: Community Cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g. mission, security requirements, policy, and compliance consideration).

Public: Cloud services are available to the public and owned by an organization selling cloud services, for example, Amazon.

Hybrid: Hybrid cloud is a composition of two or more clouds (private, community or public).

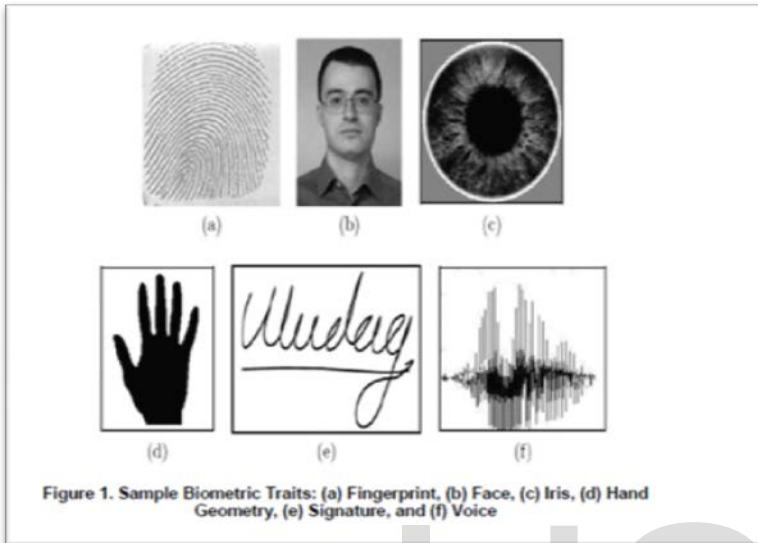
2.3 Biometrics

Biometrics is automated methods of recognizing a person based on a physiological or behavioral characteristic. The past

of biometrics includes the identification of people by distinctive body features, scars or a grouping of other physiological

criteria, such like height, eye color and complexion. The present features are face recognition, fingerprints, handwriting, hand geometry, iris, vein, voice and retinal scan. Biometric technique is now becoming the foundation of a wide array of highly secure identification and personal verification. As the level of security breach and transaction scam increases, the need for well secure identification and personal verification technologies is becoming apparent. Recent world events had lead to an increase interest in

security that will impel biometrics into majority use. Areas of future use contain Internet transactions, workstation and network access, telephone transactions and in travel and tourism. There have different types of biometrics: Some are old or others are latest technology. The most recognized biometric technologies are fingerprinting, retinal scanning, hand geometry, signature verification, voice recognition, iris scanning and facial recognition



3. Cloud Computing depended e-governance

Cloud computing is shared environment, multitenanted and over-the-internet based service delivery model. Cloud provides an attractive alternative to the common man as well as for organizations to transact and do business online. There are some key characteristics are

Accessibility: The biggest advantage of a cloud environment is its accessibility of environment by consumers. Since it is on the internet, it is always accessible. One just needs a PC and internet connectivity to access the applications. With internet becoming a fast penetrating commodity, a consumer is able access the application anywhere, anytime.

High Availability: Since the applications are hosted on internet, they need to be made available 24/7. Cloud is built on a sturdy infrastructure platform that guarantees high availability of IT infrastructure. All key components and subsystems are clustered and single point of failures eliminated. Clustering is implemented at almost all levels of hardware and even at application and middleware component levels.

Scalability: e-Governance is characterized by uncertainty in demand and load. There could be a heavy spurt in demand during particular period(s) of the year and relatively stable and lesser load during other periods. For instance, tax filing is at its peak during certain periods of the year. The platform should support adding resources

dynamically to meet this excess demand. Cloud is built on the basic premise that it is elastic and dynamic. Technologies like virtualization, clustering, and load balancing ensure scalability and high availability. Today, technologies are available to add memory and processor to the services on the fly without having to bring down either the hardware or application.

Service Orientation: Cloud is built on the concept of service oriented architecture. This facilitates provisioning of compounded or mashed up services spanning the entire consumer process keeping the end consumer in mind. At times, the model ensures ease of operation for a service receiving citizen and a service providing enterprise. This includes some of the value added services provided by external partners, on top of government services. This promotes both customer centricity and also brings in value added services and service providers to further promote the growth of e-governance.

Interoperability: e-Governance is all about multiple agencies and departments providing services to end users. With varying sets of independent applications in respective departments e-governance should make these variations transparent to the consumer. This also means that the IT infrastructure should support multiple sets and versions of applications and technologies to bring in inclusivity. Cloud computing supports interoperability as it is majorly based on virtualization and platform independent services.

Information Security: One of the key requirements of an internet based application is security as the confidential details of citizens, businesses, etc., are transacted on this platform. Though it is a multi-tenanted model, cloud provides a tight security such that confidentiality, integrity and availability of the information is not compromised. With such viable features, cloud computing is highly relevant to host e-governance applications as it guarantees reach, scalability and availability. For governments, it provides a centralized and stable platform that can be shared, re-used and can support multiple departments thereby cutting down on individual platforms and solutions.

3.1 Key elements of an e-Governance architecture

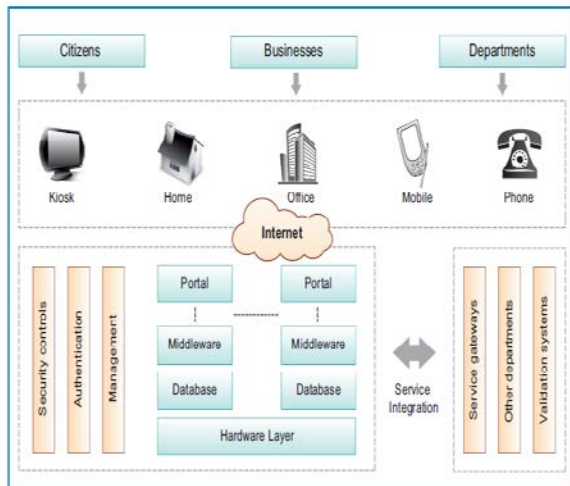


Fig: Key elements of an e-Governance architecture

3.2 Benefits of cloud computing (image from IEEE format)

Cloud Computing is having numerous advantages for end users and the business of all sizes. The huge advantage is that there is no need to have special attention towards maintenance of infrastructure & also to have experts for maintenance of the available infrastructure. The business or the people using cloud can focus mainly on their core business rather than services & infrastructure & their maintenance.

Some pros of Cloud Computing are :-

Reduced Cost: Cloud technology is paid incrementally (you pay only for what you need), saving organizations money in the short run. Money saved can be used for other important resources.

Increased Storage: Organizations can store more data than on private computer systems.

Highly Automated: IT personnel not needed to keep software up to date as maintenance is the job of the service provider on the cloud.

More Mobility: Employees can access information wherever they are, rather than having to remain at their desks.

Dynamic Scaling: Resources can be scaled up and down as per the changing needs of the business. You can add or remove storage space, memory and bandwidth using a self-service console without the involvement of the IT team.

Shared Resources: Both hardware and software resources are pooled at one location and can be accessed by all the users via cloud allowing the users to leverage the scale of economy.

Pay-as-you-go Model: Payments are calculated based on the actual time duration and amount of usage of the resources

Increased Mobility: Makes the business globally available, without any geographical constraints, as the solution is available over the cloud.

Less or No CAPEX: No huge initial investment, very less IT operational costs. It is best suited for most SMBs.

Cost Efficiency: The cloud is in general available at much cheaper rates than traditional approaches and can significantly lower the overall IT expenses. At the same time, convenient and scalable charging models have emerged (such as one-time-payment and pay-as-you-go), making the cloud even more attractive.

Convenience and continuous availability: Clouds offer services that are available wherever the end user might be located. This approach enables easy access to information and accommodates the needs of users in different time zones and geographic locations.

3.3 Table Current E- Governance Versus Cloud E-governance

Current e-Governance	Cloud Governance
Single channel service	Multichannel service
Isolated Governments	One-stop Governments
Traditional security	RBAC using fingerprint biometrics security
Respective Departments	Unified Supervision
Rigid Configuration	Dynamic Distribution
Corrupted Government	Fully transparent Government
Huge Capital Investment & Low Profit	Low Investment & Huge Profit

4. Security issues In Cloud Computing

4.1 Data Security : Encryption, fine grained authorization.

4.2 Network Security: All data flow over the network needs to be secured in order to prevent leakage of sensitive information. Traditional network security issues: Man in the middle, IP spoofing, Port scanning, Packet sniffing. Encryption techniques such as: Secure Socket layer [SSL], Transport Layer Security [TLS].

4.3 Data locality: Due to compliance and data privacy laws in various countries, location of data is of utmost importance in many enterprise architecture.

4.4 Data integrity: Data integrity is easily achieved in a standalone system with a single database. Data integrity in such a system is maintained via database constraints and transactions. Transactions should follow ACID (atomicity, consistency, isolation and durability) properties to ensure data integrity. In distributed environment, there should be central global transaction manager. Can be achieved by 2 phase commit protocol.

4.5 Data Segregation: As a result of multi-tenancy multiple users can store their data using the applications provided

by SaaS. In such a situation, data of various users will reside at the same location, so Intrusion of data of one user by another becomes possible in this environment. This intrusion can be done either by hacking through the loop holes in the application or by injecting client code into the SaaS system. A client can write a masked code and inject into the application. If the application executes this code without verification, then there is a high potential of intrusion into other's data.

4.6 Availability

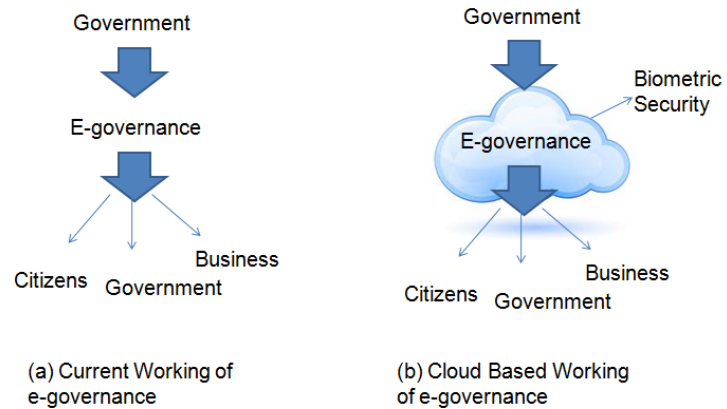
SaaS applications need to provide it's service around the clock and this will be ensured by 2 ways: Making some architectural changes at the application and infrastructural level for scalability and availability. Adopting a multitier architecture supported by a load balancer farm. Resilience to hardware and software failures and denial of service attacks. Considering an appropriate action plan for business continuity and disaster recovery. Mitigation techniques for distributed denial of service. Automatically locking user accounts after successive incorrect credentials, but incorrect configuration and implementation of some features can be used by malicious users and do denial of service.

4.7 Backup

Sensitive enterprise data should be backed up for recovery in case of disasters. Using strong encryption techniques to protect backup data.

Lack of Trust management and privacy in cloud: As it is seen in the cloud environment do not have adequate trust and privacy management facilities established well in place to mitigate the fear of cloud users in moving their critical IT business and data to cloud. Consumers and cloud service providers are forced to trust among themselves without much knowledge about the vendor's availability, back up, job service efficiency, security controls and so on. On the other

5. Proposed Scheme of Cloud & Biometric E-governance



Traditional Hosting Model	Cloud Computing Model
End user (or the customer) purchases IT assets (hardware, software, licenses, etc.) upfront and ownership of IT assets is with customer	Service provider procures the IT infrastructure and the ownership of the IT assets is with the cloud service provider
IT infrastructure hosted in a datacenter within the customer premises (or at times, co-hosted in a datacenter service provider)	IT infrastructure hosted in the cloud datacenters in the service provider premises
Whether used or not, compute resources available full time to users	Compute resources available to users on demand and for specific durations as well
No need to pay for the usage of the resources	Charged on per-usage basis
High initial investment and high on-going costs	No or very low initial investment. Reduced operating expenditure
High overheads like vendor management, server monitoring and management	Low overheads
Dedicated infrastructure	Shared infrastructure or multi-tenanted

The proposed scheme of e-governance is having following advantages

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

5. Role of Biometrics in Security

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 or behavioral traits. There are three traditional ways of authenticating the identity of an individual, these include: 1) Possessions (such as keys, passports, and smartcards), 2) Knowledge (user ID, passwords and pass phrases), and 3) Biometrics.

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 in the e-governance cloud.

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. In 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.

Key Characteristics of Cloud E-governance

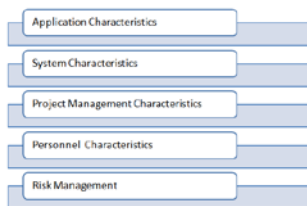


Figure : Key characteristics of Cloud E-governance

6. Conclusion

E-governance with Cloud and Iris (biometric) offers transparent and secured services to the consumers, business, government. Government can use cloud e-governance and to protect that e-governance cloud they can use biometric (Iris) recognition to secure the data from unauthorized users. This will help the user of the e-governance to maintain reliability & transparency to the e-governance users. The cloud security issues can also be solved using iris passwords.

REFERENCES

- [1] N. Santosh Ranganath, "E-GOVERNANCE AS A DEVELOPMENT TOOL FOR GOOD GOVERNANCE," *IJRIM Volume 3, Issue 1 (March 2013) (ISSN 2231-4334)*
- [2] Dr. Pardeep Mittal, Amandeep Kaur, " E-Governance - A challenge for India" *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013 ISSN: 2278 - 1323*
- [3] Sahar Mohammed Abduljalil, Osman Hegazy, Ehab E. Hassanein "A Novel Approach for Handling Security in Cloud Computing Services," *International Journal of Computer Applications (0975 - 8887) Volume 69- No.5, May 2013*
- [4] Akodiya Babubhai V., Bhavin Mathiya J., Suthar Vishnukumar H,"Cloud Computing is Marvellous Highway of an E-Governance in Gujarat State: A Study"
- [5] SET Labs Briefings Vol 9 No 2 2011 Business Innovation through Technology. Infosys
- [6] Madhavi Gudavalli¹, Dr. D. Srinivasa Kumar² and Dr. S. Viswanadha Raju, " Securing E-Governance Services through Biometrics" *International Journal of Security and Its Applications Vol.8, No.1 (2014), pp.103-112 <http://dx.doi.org/10.14257/ijisia.2014.8.1.10>*
- [7] Rajan Manro, Dr. Rajneesh Randhawa, Dr. A S Joshi," Security Issues in Cloud based e-Governance model", *International Journal of Computers & Distributed Systems, Volume 1, No.1, Jun 2012*
- [8] Mr. S.Nagaraju,Dr. Latha Parthiban,Mr. B.Santhosh Kumar," An Enhanced Symmetric Role-Based Access Control Using Fingerprint Biometrics for Cloud Governance", *Parallel and Cloud Computing Research (PCCR) Volume 1 Issue 2, July 2013.*
- [9] Peter Peer and Jernej Bule, Jerneja Žganec Gros and Vitomir Štruc," Building Cloud-based Biometric Services " *Informatica 37 (2013) 115-122*
- [10] National Information Center , "e-Governance Book 2012,"