Conceptual Framework for cloud supported E-Governance Services

Naveen Tewari[1], Dr. M K Sharma[2]

1. Research Scholar, Bhagwant University, Ajmer, Uttarakhand, India, E-mail: navtewari@gmail.com
2. Associate Professor, Amrapali Institute, Haldwani, Uttarakhand, India, E-mail: sharmamkhld@gmail.com

Abstract: *The focus of this paper is to develop an architecture using cloud for e-governance. Cloud computing offers an easy means of achieving the application model of e-Governance with multi-tenancy. We can use public Internet as a type of communication medium and provide a framework, which can be used by every citizen in spite of his or her diversity & location. This model combines SaaS, PaaS, IaaS and SWAN (State wide area network) architecture.*
This model also gives the detailed level architecture of SaaS, PaaS, IaaS and SWAN individually.
Index Terms: *Government, e-Governance, Internet, NeGP, Government Services, e-Governance Projects, Citizen, Cloud, Cloud deployment model, SaaS, PaaS, IaaS, cloud security, SWAN, SDC, CSC, SSDG, NSDG.*

I. INTRODUCTION

This paper aims to propose a new theoretical/mathematical framework for e-governance using cloud computing. This paper will also analyze the pre-requirement to offer e-governance through cloud computing. We will discuss/design a prototype for the proposed architecture. This paper will propose the power of cloud computing to be integrated into e-governance framework.

The proposed architecture *figure 1* describes the overall architecture of the e-Governance framework using cloud computing. This architecture contains all the three level of Cloud (IaaS, PaaS & SaaS) connecting with a common networking facility provided by the government.

II. CLOUD COMPUTING IN E-GOVERNANCE

E- Governance is facing some challenges and cloud provides the way to cope up with these challenges. So here we provide the challenges and their removal process as described by cloud.

Cloud is used as an umbrella term to describe a category of sophisticated on-demand computing services offered by some commercial providers [16]. Through cloud on-demand, A-Z computing experience can be given to citizens (customers). This gives numerous benefits to the user and provides various facilities under one roof. Cloud can also be integrated in ongoing e-governance projects and, enlarge them by incorporating various cloud services. This, feature makes cloud best choice for all professionals [16].

III. E-GOVERNANCE FRAMEWORK USING CLOUD COMPUTING (PROPOSED MODEL)

We have seen various deployment models of cloud, our proposed model will work on hybrid model. Hybrid is the combination of two or more deployment models; here private and public model constitutes the proposed hybrid model as the model of deployment. We will describe the proposed model as the combination of different layers.

IaaS Layer: IaaS layer will comprise of the Infrastructure needed for the PaaS. This layer is strictly owned by government agencies. So, it will act as a private cloud. Government data is highly secured and cannot be given to third party IaaS provider. Therefore the IaaS architecture is to be developed within Government premises. Various facilities provided by the IaaS as needed for PaaS layer are:
- Data Storage
- Networking
- Load Balancers
- Virtual Environment
- Various servers like Database Server, Application Servers, and Web Servers etc.

The first and foremost need is the Storage centre. The needed storage is provided by the SDC (State Data Centre) already working in almost every State and Union Territory of India. These SDC's are connected with very high bandwidth of networking model known as SWAN (State wide area network). Under SWAN scheme, technical and financial assistance are being provided to the States/UTs for establishing SWANs to connect all State/UT Headquarters up to the Block level via District/ sub-Divisional Headquarters, in a vertical hierarchical structure with a minimum bandwidth capacity of 2 Mbps per link [7]. Each of the State / UT can enhance the bandwidth up to 34 Mbps between SHQ and DHQ and up-to 8 Mbps between DHQ and BHQ depending upon the utilization [7].
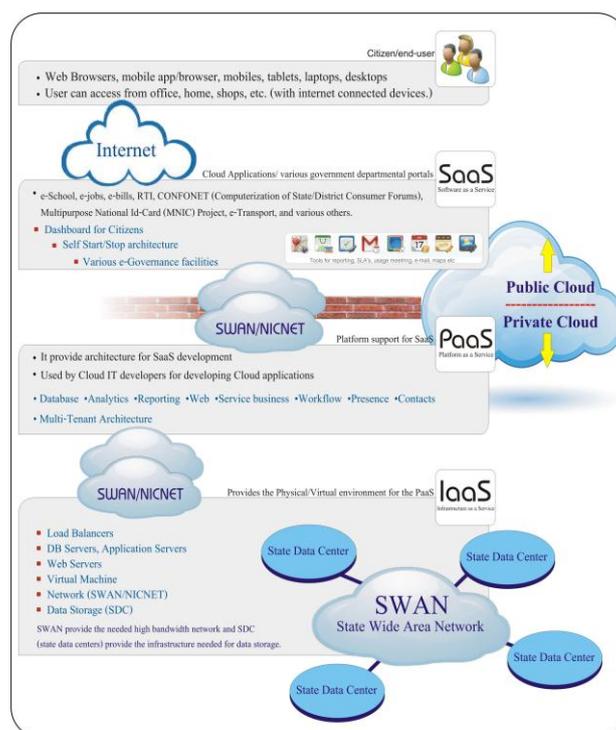
Figure 1: e-Governance Framework using Cloud Computing

We have connected this SWAN model to our IaaS layer for providing Data Centre and Networking. We are also using this networking model to connect IaaS to PaaS and further SaaS. This existing infrastructure will prove as a backbone to our model. This also lower down the cost of implementation as already it is implemented in every State and Union Territory in India [7].

IaaS will work on a virtual environment for providing the multi-tenant support. Load Balancer will use virtual platform for providing this feature. Various virtual servers are available in the market. Virtual server is used create the virtual image of computing resources like Operating Systems, Network, Application servers, Web servers, memory, etc. This will create a layer through which the user interacts with IaaS. Different virtual images with different resources discussed above are created for all users (multi-tenant), which is not possible in physical system.

PaaS Layer: The next step is to connect PaaS to IaaS through SWAN. PaaS will provide the necessary development platform for Software as a service (SaaS). The different facilities provided by PaaS are:
- Operating systems images (provided by IaaS) like Microsoft Azure etc.
- Various Languages needed for cloud application development like PHP, JAVA etc.
- Various databases like mySQL, SQL server etc.
- Workflow
- Multi-tenant architecture

These facilities are needed by the cloud developer for developing cloud base working applications. PaaS platform only provide the platform as a service so it can be deployed as public as well as in private cloud. But, for better controlling of cloud at government level this can be deployed as private cloud.

SaaS Layer: SaaS is also connected to PaaS by SWAN architecture already present. It provides a presentation layer framework for citizen/end-user. Software developed at PaaS level will be provided to the citizen at this level. Various cloud based government portal can be developed for the citizen.

Various facilities provided to the citizens are:
- Government portal for cloud based governance
- G2C, G2G, G2B facilities can be provided through SaaS
- User friendly dashboard to the user providing the following feature
  - Self Start/Stop Service
  - Various facilities like e-mail, feedback etc.
  - Usage metering

SaaS will only provide the required software as a service therefore it will be implemented through public cloud deployment model. SaaS will interact to PaaS and IaaS with the help of local intranet present at government level known as SWAN (State wide area network).

We have discussed SaaS in detail further in this chapter.

Citizen/end-user: Citizen or end-user will be connected to our cloud model with the help of internet. Citizen will be directly connected to SaaS with the help of webURL provided by Government SaaS provider. Citizen will have to sign an SLA with the SaaS provider which will provide the security features and necessary terms and conditions between them.

Citizen can access the SaaS service with their devices like laptop, desktop, PDA, tablet, mobiles, provided the internet connection should be there. They can access the services in their office, home, or anywhere where the internet service is available.

Various service citizens are able to use as a service are:

- Land Records
- Birth/Death Certificates
- Grievances
- Form downloads and submissions
- Bill payments –water, electricity, telecom, etc.
- Licenses, permits, subsidies
- Property Tax and Registration
- Bus pass, Railway tickets, Passport, etc.
- Health services
- E-Commerce, Commercial services, and many more

These services are developed by cloud (SaaS) developers (public/private) based on the platform at PaaS level and infrastructure provided at IaaS level. All these level accept end-user will be connected via SWAN architecture.

All the data gathered through SaaS will stored in SDC (State Data Centre).

Government will sign MOU and SLA with cloud provider at each level whether it is private level (IaaS/PaaS) or public (PaaS/SaaS).

Security is the main concern in this architecture and we will discuss this feature with others in detail at further level in this chapter.

We will also discuss the will be used technologies for the architecture, whether software, hardware or languages.

IV. E-GOVERNANCE FRAMEWORK FOR SaaS (PROPOSED MODEL)

We are proposing a SaaS framework for e-Governance that will define the detail overview of why & how citizen will interact with the SaaS services and how cloud SaaS provider and Government are linked with this architecture.

Cloud SaaS framework includes the following:

Use case model based on the working architecture of SaaS that provide detail overview of users and services used by them.

Working model/reference architecture to give the basic idea of SaaS in e-Governance implementation. *Layered architecture* that will give the view of required components in a SaaS application.

This architecture also defines the details required for communication with SaaS provider and further to the government.

SaaS has been proved as the major consideration among the cloud developer as it has direct engagement with the user/citizen. Applications developed at this stage are provided as a service to the citizen. These software applications are provided for free or can be given as rented/pay-as-you-go model. This model is also called as on-demand software applications.

Various features supported by SaaS applications are:

Multi-Tenancy: SaaS applications most typically support many unique customers using a single instance of that application– also known as multi-tenancy.

Security and Privacy: These are the main concern for any user as Government data is very much sensitive, various measures are provided by the SaaS provider in this area.

Scalability: Scalability is also a main feature of any SaaS application. Wide and narrow growing as needed by the citizen should be there in application.

Billing and metering: If the service is not offered for free than there is a need of billing and metering of the usage at user/provider end.

User Interface: Interface of the application should be good and easy to use. Today, SaaS applications are developing in such a way that they are more-or-less customized by the user. Like the font size, color etc. of the software. These applications are also known as 'skinnable' software.

4.1 USE CASE MODEL FOR e-GOVERNANCE SAAS FRAMEWORK

This model figure 2 is a part of our proposed e-Governance cloud architecture. In this model we have shown as how the system behaves from user centric view. There may also be other users but we have focused only the main users through which the data travels in the system. There are three such users' exist citizen, Govt. IT administrator and SaaS provider.

4.1.1 Citizen/end-user: Primary user is individual citizen who uses SaaS application for the e-governance services. These citizens are geographically disappeared from each other and use SaaS application from public domain with the help of internet connected devices.
Citizens use these applications to start/stop/consume services. They can create/read/update/delete their accounts in these government portals.
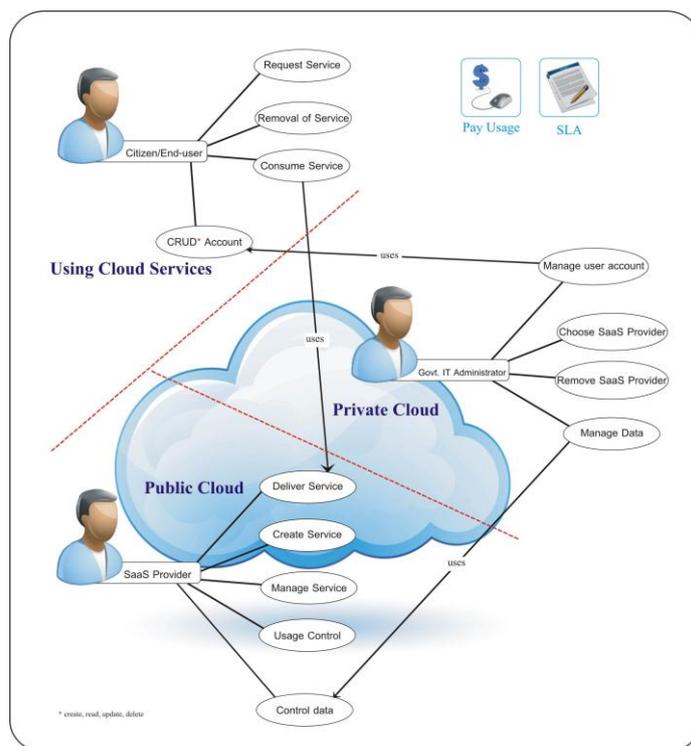
Figure 2: e-Governance SaaS Framework Use Case Model

4.1.2 SaaS Provider: These are the external service provider that delivers the software as a service over the internet. Government recruits these providers to provide SaaS applications.
These providers can create/manage/remove service as suggested by the Government. They can also able to deliver service to the citizens as requested and manage their usage control. SaaS provider also acts as a mediator in between Government and Citizen. Data is being controlled and sent to the government data centre by these service providers. These provider work from public cloud and are provided with the facility to connect to government private cloud.

4.1.3 Government IT administrator: These are the user at government end. Therefore they always uses private cloud platform. These Government IT Administrators (Specialist) are responsible to choose/remove a competitive SaaS provider. They also provide the required PaaS platform (private/public) for SaaS provider to develop their applications. They also manage user Accounts and their data as they have the privilege to access the required data centre present at government IaaS level.

These users are bounded by a well defined SLA for the necessary terms and conditions. Usage control also managed at SaaS provider and government level for better and transparent controlling.Data is exchanged at public/private cloud layer. Both the layers are well connected by high internet connectivity provided by SWAN

(State wide area network). How PaaS will provide a platform for SaaS and the connectivity model for SWAN will be discussed further in this chapter.

4.2 REFERENCE/WORKING ARCHITECTURE OF e-GOVERNANCE SAAS FRAMEWORK
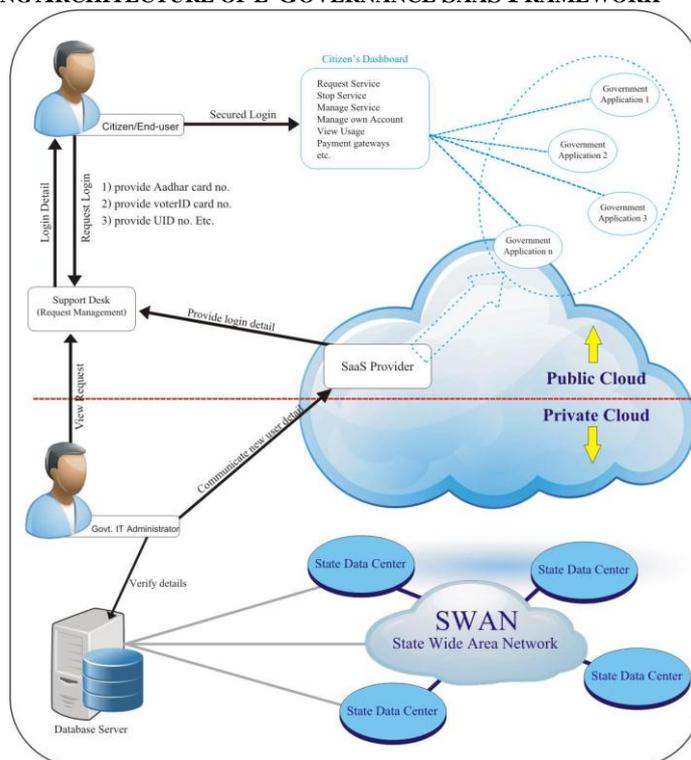
Figure 3: e-Governance SaaS Framework Reference/Working architecture

This architecture *figure 3* provides the basic working flow model of SaaS Architecture. It consist interchange of data, data management and interaction of public and private cloud.

Workflow of the proposed architecture:
1. *Citizen login to the system*
2. *Authentication Check*
    a. *If user exist then move on to Citizen's dashboard at step 3*
    b. *Else citizen request login detail*
        i. *Citizen provide its identification to support desk (identification should be a government provided card number)*
        ii. *Government IT administrator view request at support desk*
        iii. *IT Administrator check the given detail from database server connected to SWAN (State wide Area Network) & SDC (State data centre)*
        iv. *If the details given are correct then login detail generated and provided to SaaS provider.*
        v. *SaaS providers manage the login detail according to their application and provide the detail to citizen via support desk.*
        vi. *Citizen get the details and securely login into the system*
3. *Citizens gets the following facility in its Dashboard*
    a. *Request Service*
    b. *Stop Service*
    c. *Manage Service*
    d. *Manage own Account (Change password etc)*
    e. *View Usage*
    f. *Payment gateways*
    g. *Etc.*
4. *Citizens also get facility to interact with various government portals provided by SaaS provider from dashboard.*

Data interchanging in this architecture is of the main concern. SaaS provider is a third party vendor and government data must be secure in-between the transaction. There must be synchronization between the external and internal system. As Citizen's information is kept at public and private level so data must be kept in encrypted format. We also have to identify the security breaches in the transmission of data from public to private cloud and vice-versa.

4.3 LAYERED ARCHITECTURE OF E-GOVERNANCE SAAS FRAMEWORK
        The layered architecture provides the different distributed tier of a SaaS application. These distributed layers/tiers are:
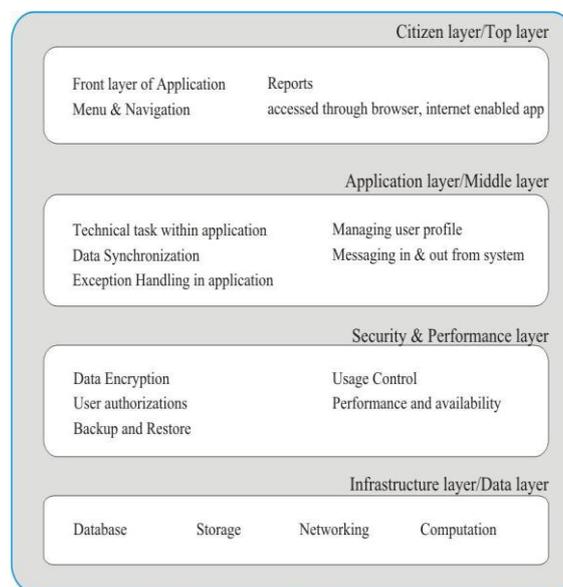
Figure 4: Layered architecture of e-Governance SaaS Framework

4.3.1 Citizen layer/Top Layer: This tier has the presentation end of the software. This end provides the front panel exposed to the citizen. This usually contains the web browser installed for free on various devices.
Menu/navigation: Citizen gets the access to features and facilities through these menus and navigations.
Browser Accessibility: Citizen can get the services in a device that support browser or an application that will give proper support to internet.
Reports: User gets the desired report from an application so they can keep record up-to-date.

4.3.2 Application layer/Middle Layer: The application layer or middle tier consists of the technical aspect of the application i.e.
Data synchronization: Synchronization between the data of an application and external data should be present in this tier.
Exception handling: Run time error management is known as exception handling. This is how the application exposed to user in case of error occurring.
Managing user profiles: User profiles are should be managed through application. This facility should be given to citizen to manage its account up-to some limitation.
Messaging in and out from the system: Messaging to outer world from an application is the old and important way of communication. This should be present in every application of SaaS model. Application should be able to communicate to citizen, SaaS provider, Government etc for proper working of the system.
The application tier generally provided such application services as clustering of application servers and load balancing between them for scalability and resilience, management of user session data, management of database connection pools and management of application objects containing business logic [8].

4.3.3 Security & Performance layer: This layer contains the security and performance measures of the model.
Data encryption: Data encryption provides the high level of security and should be available in every interchange of data to and from the system.
User authorization: Individual access to the system should be provided after the authorization has been confirmed.
Availability: Availability represents a percentage of how much of time the application is available to the user.

Backup & restore: In case of system failure due to some natural disaster like floods etc. there must be a provision of backup of data and restoration of facilities. This is one of the main advantage of Cloud computing.
Usage control: User must be aware of what they are using and the time duration of services. This is accomplished by usage control. This also gives the feeling of transparency to the citizen.
Dynamically scaling the application according to user requirement is controlled at this tier.

4.3.4 Infrastructure layer/Data layer: This constitutes the physical layer on which the data resides before moving to the IaaS layer. In some cases this is the actual IaaS layer. But in our model this is the virtual layer in the public cloud and connected to private cloud through SWAN. The data then is moved to IaaS layer. This layer also provides the virtual network, virtual computing etc. required for the working of SaaS applications.
Database: As we know that cloud enables multi-tenant architecture, so as its database. Database should be present for all tenants independently or the same database is shared to all tenants maintaining their identity.
Network: Same as the database network is also shared by all tenants. As our architecture uses government network model known as SWAN (State Wide Area Network), the same must be virtualized to support multi-tenant architecture.
Storage: We are giving this model for the betterment of government services. So storage must be shared securely and privately between the tenants. SDC (State Data Centre) provide the required architecture support for storage.
Computation: The necessary virtual servers, web servers etc. provide the computation facility to the model.

V. ARCHITECTURE FOR CONNECTING CLOUD FRAMEWORK TO SWAN
For understanding/visualizing the cloud connectivity to SWAN, firstly we have to understand NeGP (National e-Governance Plan).

5.1 NEGP (NATIONAL E-GOVERNANCE PLAN) [9]
The NeGP aims at improving delivery of Government services to citizens and businesses with the following vision: "Make all Government services accessible to the common man in his locality, through common service delivery outlets and ensure efficiency, transparency & reliability of such services at affordable costs to realize the basic needs of the common man [9]."

Infrastructure of NeGP
The infrastructure pillars of NeGP are:
Connectivity: State Wide Area Networks (SWANs)/NICNET
National Data Bank/ State Data Centres (SDCs)
Common Service Centres (CSCs) primary mode of delivery

5.1.1 SWAN (State Wide Area Networks)
SWANs across the country, when fully implemented, will create more than one million routes – km of network connecting more than 100, 000 government entities. Success of various e-Government initiatives taken up at the State and the Central level would heavily depend on maximum utilization of SWANs [9].

Key Infrastructure – Features (SWAN) [9]
- Minimum 2 Mbps connectivity till Block level
- Over all project outlay of Rs. 3334 Crore including State share.
- Around 7500 POPs and provision of Data, Voice and Video connectivity services to more than 100,000 Government offices.
- Two Implementation Options:
  - Option I : Public Private Partnership (PPP)
  - Option II : NIC (National Informatics Center)
- BSNL- Primary Bandwidth Service provider.
- Service Based Implementation and Operational Framework.

5.1.2 State Data Centre (SDC) [9]
State Data Centre (SDC) is created for a shared secure resource for consolidation of Data, Services, Applications & Infrastructure at the State/UT level to enable electronic delivery of G2G, G2C & G2B services. It also needed for optimal utilization by sharing of IT Infrastructure Resources to meet individual peak loads. The State/UT and NIC together will form a composite team for the State Data Centre.
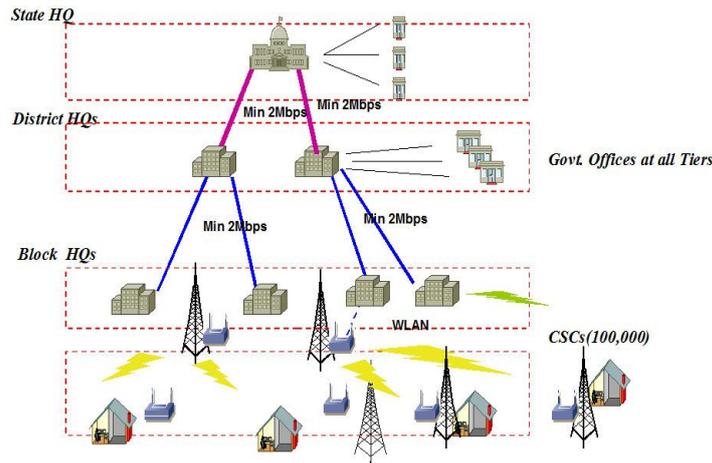
Figure 5: SWAN Architecture [9]

5.1.3 Common Service Centres (CSC) [9]

The purpose of Common Service Centres is to create a low cost vehicle for Government institutions so that easy, direct and cost-effective delivery of e-Governance services to the rural citizen is possible. The aim is to create 1, 00, 000 CSC across the Country at the village level.

5.1.4 National e-Governance Service Delivery Gateway (NSDG) [9]

The National e-Governance Service Delivery Gateway (NSDG) provide a standardized interfacing, messaging and routing switch through which various players such as departments, front-end service access providers and back-end service providers can make their applications and data inter-operable [9].
The National e-Governance Service Delivery Gateway (NSDG) aims to achieve a high order of interoperability among autonomous and heterogeneous entities of the Government (in the Centre, States or Local bodies), based on a framework of e-Governance Standards [9].

5.2 PROPOSED CLOUD AND SWAN ARCHITECTURE
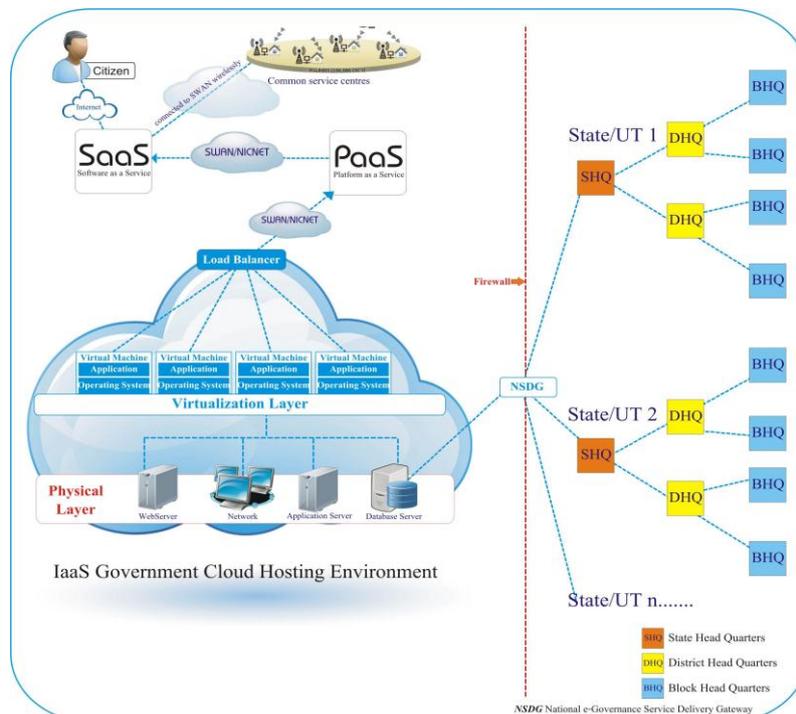
Figure 6: CLOUD connectivity with SWAN

The above *figure 6* describes how cloud can be connected SWAN network of e-Governance. This is the proposed conceptual architecture of connecting Cloud to SWAN. We are giving emphasis to this model because it will reduce the task of developing the data storage centers and high speed network connections for cloud

based e-governance. These are already implanted and in working condition in the form of SWAN as discussed in section 5.8.1. This will also reduce the cost of Cloud implementation and installation.

In this proposed model SWAN (see section 5.8.1.1) provides a communication/interface medium known as NSDG (see section 5.8.1.3) to outer world/departments. We are taking this as the core facility provided by the Government.

We are connecting NSDG to IaaS platform developed and maintained in-house (Government level) for implementing private cloud.

At its core, infrastructure as a service is a way for organizations to get the hardware, storage, networking and other services they need to run their operations without worrying about buying, managing or maintaining the equipment. With this model, Government "rent" the equipment, paying only for the capacity and space they use [10].

But implementing and maintaining the cloud in-house provides more security to sensitive Government data and services. Therefore, we are proposing the private IaaS model. In this model all the needed hardware, network resources, servers, web services, IaaS software are purchased and implanted at government level and maintained by Government IT professional / Government agencies like NIC (National Informatics Centers) etc.

Moving further, NSDG provide the connection between various State level Data Centers through a common gateway to IaaS database servers. Various Servers like database servers, application servers, web servers, network, web services etc are connected to each other. Next layer is the hypervisor level providing the concept of virtualization. All the resources are connected to virtual layer, which provide the necessary resources pooling for multi-tenant architecture supported by Cloud. This will also provide dynamically scaling as needed.

Hypervisor allows multiple OS (Virtual machines) to run simultaneously on a single physical host.

PaaS will utilize the SWAN network to connect to load balancer at IaaS. PaaS will provide the necessary software architecture to develop the cloud software. PaaS can be at Public/Private cloud as needed by the Government. PaaS platform can be developed easily within the Government premises, or can rent from a third party provider in pay-per-use mode. All the application developed at PaaS level resides over the private virtual environment provided by IaaS.

Again SaaS will connect to the PaaS through SWAN architecture. This will provide the service delivery model through which services as web application are provided to citizens. These services are hosted in cloud environment provide by PaaS. SaaS will also provide facilities such as usage control, user control, metering etc.
SaaS facilities are consumed by citizens through their internet enabled devices. They can access these services through public cloud at office, home, shops, or wherever they want. SWAN also plays an important role in the facility also. Government have developed/developing around 1, 00, 000 CSC across country. These all are at Block level/Village level and connected to SWAN through Wi-Fi. These common service center (Citizen Service Center) can be used to provide Cloud services to those citizens who not able to consume these services by their own.

At each level of cloud connectivity (IaaS, PaaS or SaaS) a firewall will be utilized to provide safe and secure connectivity (Network/data) to the citizen and government.
In these models IaaS and PaaS will use private cloud whereas SaaS will be delivered through public cloud. This will contribute to hybrid cloud model.

VI.   PaaS FRAMEWORK FOR E-GOVERNANCE
PaaS Platform provides an abstraction layer between the software applications (SaaS) and the virtualized infrastructure (IaaS). PaaS offers services to software developers. Developers can write their applications according to the specifications of a particular platform without needing to worry about the underlying hardware infrastructure (IaaS). Developers upload their application code to a platform, which then typically manages the automatic up-scaling when the usage of the application grows [11]. Examples are the Google App Engine, which allows applications to be run on Google's infrastructure, and Salesforce's Force.com platform.

The PaaS layer of a Cloud relies on the standardized interface of the IaaS layer that virtualizes the access to the available resources and it provides standardized interfaces and a development platform for the SaaS layer.
Various providers from the IT Industry provide the PaaS platform. These are easy to deploy, manage and use. Some of them are VMWARE, SaaSGRID, CUMULOGIC, CLOUDBEES, IBM, ORACLE, MICROSOFT, AMAZON etc.

Government with existing infrastructure (SWAN, SDC, CSC, NSDG) can meet the challenges of delivering web-oriented, data-intensive applications while making the transition to cost-effective, elastically scalable virtual and cloud environments and protecting enterprise IT investments in legacy applications and infrastructure. This is possible because PaaS can be implemented by basically layering software onto the existing infrastructure [12].

We are explaining one of the PaaS platform architecture which can be used in our e-Governance model with some modification.
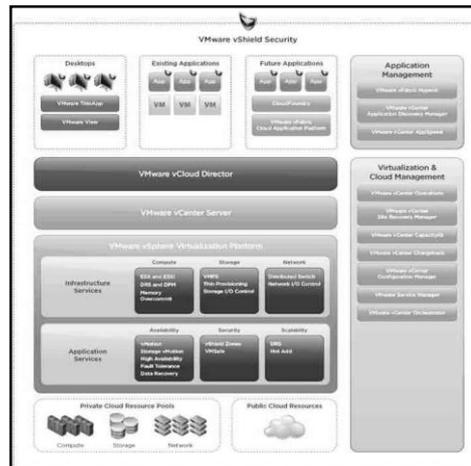
Figure 7: VMware PaaS Platform Architecture Diagram [12]

Virtualized and shared hardware infrastructure is a core requirement of this model. We are discussing these features in Government IaaS model in later section of this chapter. A private cloud and PaaS platform builds on top of this virtualized hardware infrastructure.

Here we are giving example of VMware's vCenter's Cloud platform, which can virtualize existing heterogeneous hardware infrastructures. Its vFabric or Cloud Foundry application platform provides a PaaS infrastructure for Java virtual machine (JVM) applications [12].

Cloud Foundry is VMware's open PaaS, with support for multiple frameworks and languages, and a choice of cloud platform and application services. It is a distributed system designed to allow a developer's application and associated services to take center stage while abstracting away complex middleware software infrastructure. Cloud Foundry also provides vFabric application Platform, a lightweight runtime platform optimized for modern applications running in cloud and virtual environments [12].

As seen in Figure 7, the system takes care of load balancing and availability for all application instances. Applications that fail for any reason are restarted automatically, and multiple instances are load balanced from the router pool in real time. Scaling up and scaling down is fast and efficient, allowing a developer or administrator multiple options for scaling and high availability [12].

Access to services, and binding application to services, is simple and straightforward, allowing different design patterns to emerge for the application developer. Application and service-level security can range from multi-tenant with process; file system and user-level isolation, to full hypervisor-level isolation. Developers leave behind complexity and stay focused on applications, not infrastructure or middleware [12].

Metric	Platform support
Provisioning	UI based self-service
Multi-Tenancy	Yes
Auto-Scaling	Policy based auto scaling. Scale-up, -out, and - down
Billing	Based on metered usage
IaaS Providers	Vmware
Security	Policy driven, Support for LDAP
Migration and Backup	Yes
Operating System	Support based on IaaS provider
Development Language & Framework	Java, Spring, Groovy & Grails, PHP, cloud foundry support ruby, Rails & Sinatra, Scala, Node.js
Databases	MySQL, MongoDB, Redis
Development Status	VFabric-Production, Cloud Foundry-Beta
Open source	Yes-Cloud Foundry
Hardware based appliance	No

Table 1: VMware Cloud Foundry PaaS Services [12]

There is numerous other PaaS provider available. So, here government has to be careful in evaluating and choosing a PaaS provider. Government will also have to check the planned SaaS applications and their compatibility with the chosen PaaS.

As seen in Table 5.1 VMware is supporting large Amount of languages and databases, so it has to be checked whether the government IT professionals are ready to work on these platform as provided by the provider.

Governments will also check for the data center compatibility with the PaaS platform. Careful consideration must be given to topics such as where the organization stands relative to adopting shared infrastructure services.

VII.   E-GOVERNANCE FRAMEWORK FOR IaaS
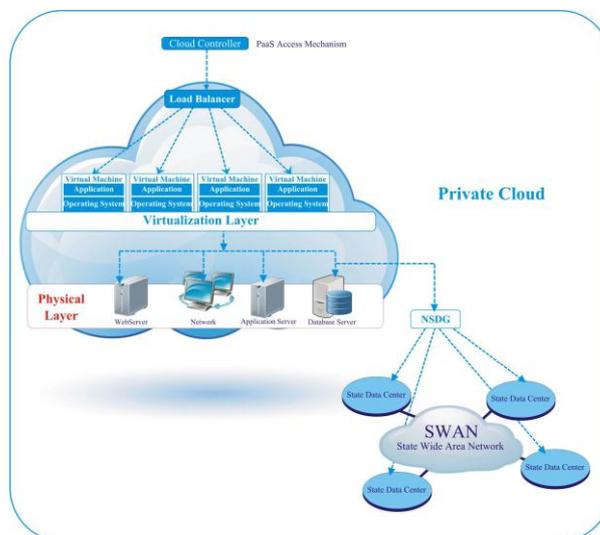
Figure 8: Private IaaS model for e-Governance

Our proposed architecture of IaaS e-governance consists of several components of cloud design and SWAN model. We have infrastructure building blocks like storage, network, and computation as well as state data centers (SDC) provided by NeGP. This architecture gives the basic idea of how the SWAN and IaaS be clubbed to provide the necessary infrastructure elements of cloud.

The State Data Centers provide by government and connected through SWAN contains the citizens data and other information needed for government applications and services. As we have discussed this setup has already been provided by the government.

NSDG provides the outer link of this SWAN network with SDC. So through NSDG we connect our database servers to the SWAN and SDC. Database servers in IaaS provide the storage for applications, web services, and other resources. These also works as a slave databases getting the desired confidential data through SDC over a confidential identity. The private IaaS model dedicates the computing, storage and network resources to the government premises. It will be delivered and installed in government data center location behind the firewall.

This private model of cloud provides a high level of security which is always the main concern of any government department.

IaaS model will provide a physical layer which will define all the physical resources like networks, servers (application server, web server, OS, database server, storage etc [13]. This layer is made available to PaaS for application development through a virtual layer.

Virtualization provides the multi-tenant infrastructure in the form of virtual machine (VM). This enables multiple applications, owned by different government department (developed through platform provided by PaaS), to transparently share common underlying physical resources, such as servers and storage [14]. Rather than purchasing physical servers, software, data center space, and network equipment, government departments will receive these resources as VMs [14].

Virtualization results in higher efficiency, utilization and lower cost as it enables hardware resources to be shared and pooled across multiple applications. It also provides the ability to grow and shrink according to the user need. Load balancing is also possible through virtualization.

Virtual machines enable far more detailed accounting of which applications, LOBs, customers are using IT resources i.e. usage billing and invoicing can be done with the help of virtualization more easily.

Various Virtual machine available in the market are e.g., VMware, AMD, BEA Systems, BMC Software, Broadcom, Cisco, Computer Associates International, Dell, Emulex, HP, IBM, Intel, Mellanox, Novell, QLogic, and Red Hat etc.

Load Balancer is the Cloud controller which is actually a management program that enables the entry point to PaaS developer. It manages the request from different users from outer environment (like PaaS developers) other than IaaS.

Networking in the model constitutes both inner and outer level. These both level networking is provided by the SWAN network. SWAN provides the necessary infrastructure needed for network resources at physical layer. SWAN is used at state level Cloud as well as national level cloud. SWAN network is also used to connect IaaS to PaaS model. It consists of two gateways NSDG (National Service Delivery Gateway) for National network and services and SSDG (State Service Delivery Gateway) for State network and services.

VIII. CONCLUSION & FUTURE WORK

Our proposed architecture will give a roadmap for providing e-Governance services through Cloud computing. Hybrid model (private + public) will provide a sense of security to both at government and citizen level. After implementing this model, we expect that the cloud will become suitable for hosting highly demanding, mission-critical government applications.

The network and data store are the foundation of cloud computing. The cloud services simply cannot be delivered without the network and its ability to monitor, manage, and report. Government SWAN and SDC will act as a backbone infrastructure for cloud and we have integrated it with the IaaS model.

Security is one of the main issues as faced in cloud implementation. The future work will be based on the security and other concerning issues of cloud computing.

Benefits and other issues will also be discussed in the near future.

REFERENCES

[1]   "Business Innovation Through Technology" e-Governance, SETLabs Briefings, Vol 9 - No 2, 2011
[2]   (2009)Wikipedia The free Encyclopedia [online]. Available: http://en.wikipedia.org /wiki.
[3]   Sameer Sachdeva," E-Governance Strategy in India", White Paper on E-Governance Strategy in India, December'2002
[4]   "Cloud Computing for E-Governance", A White Paper, IIIT Hyderabad, January 2010 , http://search.iiit.ac.in/uploads/CloudComputingForEGovernance.pdf
[5]   Naveen Tewari, Dr. M K Sharma, "Cloud based Working Concept for E-Governance Citizen Charter", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 3,Issue 6,June- 2013
[6]   http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf accessed on December 2014
[7]   http://deity.gov.in/content/state-wide-area-network-swan accessed on December 2013
[8]   "Business making progress", © 2008-2009 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved, Rev. 11/09 | 6525-128713, www.progress.com/worldwide
[9]   "Transforming Government – e-Government Initiatives in India", Editors: R K Bagga and Piyush Gupta, Published by: The ICFAI, University Press, 2009.
[10]   "Infrastructure as a Service", A white paper, ISO 9001:2000 certified 108289 -120702, ©2012 CDW LLC
[11]   RightScale (2008) Define Cloud Computing. RightScale Blog, 26 May 2008. http://blog. rightscale.com/2008/05/26/define-cloud-computing/. Accessed: december 2013
[12]   A whitepaper on "Cloud computing and Platform as a service - leveraging the benefit s of paas and private clouds", © 2011 Compuware Corporation
[13]   A whitepaper on "Virtualized Multi-Tenant Data Center Solution for Infrastructure-as-a- Service", C11-604559-01, 09/10, printed in USA, © 2010 Cisco and/or its affiliates. All rights reserved.
[14]   IT@Intel White Paper, "An Enterprise Private Cloud Architecture and Implementation Roadmap", Intel Information Technology, Business Solutions, June 2010
[15]   Michael Glas & Paul Andres, "Achieving the Cloud computing vision", Oracle whitepaper in Enterprise Architecture, October 2010.
[16]   Naveen Tewari, Dr. M K Sharma, "ARCHITECTURE OF E-GOVERNANCE CITIZEN CHARTER USING CLOUD", International Journal of Information Technology & Computer Sciences Perspectives © Pezzottaite Journals., Volume 2, Issue 3, July-September 2013
[17]   http://en.wikipedia.org/wiki/Service_quality#cite_ref-1 as accessed on 30/11/2013
[18]   Wendy Ginsberg, Maeve P. Carey, L. Elaine Halchin, Natalie Keegan, "Government Transparency and Secrecy: An Examination of Meaning and Its Use in the Executive Branch", November 14, 2012, Congressional Research Service, 7-5700 ,www.crs.gov ,R42817
[19]   Puneet Kumar, Dharminder Kumar, Narendra Kumar, "Improved Service Delivery and Cost Effective Framework for e-Governance in India", International Journal of Computer Applications (0975 – 8887), Volume 74– No.2, July 2013
[20]   http://indiagovernance.gov.in/e-governance.php accessed on 04/12/2013
[21]   Implementing e-governance reforms , "Promoting e-Governance – The SMART Way Forward"
[22]   Subhajit basu, "e-government and developing countries: an overview", international review of law computers, & technology, volume 18, no. 1, pages 109–132, march 2004
[23]   http://apit.ap.gov.in/index.php/e-gov accessed on 05/12/2013
[24]   "Public-private partnerships in e-government: knowledge map", an infodev publication prepared by: the institute for public-private partnerships, june 2009
[25]   Caroline J. Tolbert, Karen Mossberger, "The Effects of E-Government on Trust and Confidence in Government", Public Administration Review , May / June 2006
[26]   http://www.rickscloud.com/cloud-computing-enables-business-scalability-and-flexibility/ accessed on 17/12/2013
[27]   Naveen Tewari, Dr M K Sharma, "Security Issues Of Cloud Computing - An Analysis", 17th Annual Conference Of Gwalior Academy Of Mathematical Sciences And National Symposium On Computational Mathematics & Information Technology, 7-9 December 2012, at Jaypee University of Engineering & Technology, Guna, MP
[28]   http://searchcloudsecurity.techtarget.com/tip/Cloud-computing-access-control-Access-management-services-in-the-cloud as accessed on November 2013.
[29]   http://www.techopedia.com/definition/26802/vendor-lock-in as accessed on December 2013