Working Group Report on Cloud Computing Option for Small Size Urban Cooperative Banks

Index

Working Group report on Cloud computing option for Urban Cooperative Banks

Executive summary

Working group for exploring use of Cloud Computing option for small size Urban Cooperative Banks was set up by RBI comprising senior officers from the Reserve Bank of India, experts from the software industry and eminent professors from academia. The working group reviewed the profile of the sector, technological trends in Cloud Computing and use of cloud like solutions within UCBs. Based on the analysis, the working group has suggested its approach for Cloud computing option.

2. RBI had already identified minimum IT support for front office and back office operations, MIS and Regulatory reporting. Though there has been a good progress particularly in banks having five and more branches which covered nearly 60% of the total banking business provided by the UCB sector, large number of banks having up to five branches still did not have core banking solutions. This segment of the sector is also characterised by absence of technical manpower, small size and low level of banking complexities.

3. The National Institute for Standards and Technology (NIST) has defined cloud computing as, "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The NIST has proposed reference architecture for cloud computing wherein the IT services are provided as Infrastructure as Service (IaaS), Platform as service (PaaS) and software as a service (SaaS) with increasing level of abstraction for the cloud customer. It identifies the Cloud Provider, Cloud Consumer, Cloud Auditor, Cloud Broker and Cloud Carriers as the players in cloud computing and Private Cloud, Community Cloud, Hybrid Cloud and Public Cloud as deployment models with increasing level of service options but also increasing security concerns. The cloud model therefore is composed of five essential characteristics, three service models, and four deployment models. As target banks have limited technical skills and lack of or little software solutions, SaaS model could be suited for them. NIST has identified Open issues in cloud computing as Computing performance, Cloud reliability, Attainment of Economic goals, Compliance with regulations and Information security. The NIST has also identified Process and Technology oriented security concerns in cloud

computing. The Information Systems Audit & Control Association (ISACA) has suggested six guiding principles, control objectives and framework as well as Audit scope for cloud environment.

4. Study observed that many Urban Cooperative banks have been providing IT support to other cooperative banks which included sharing of Data Centre and DR sites, Automated Teller Machines, Payment gateways. Some of these banks were also providing their software solutions as outright sale or fees based ASP model. It was observed that two leading software firms had been also offering cloud like services which included core banking as well as many other solutions such as HR solutions, e-mail, storage, etc which the banks could choose. These services were mostly on private cloud like set up.

5. As both Bank provided as well as Software Developer provided cloud like solutions are in use among the Urban Cooperative banks, such solution provide an opportunity for further use. However, most of the open issues and security concerns are still not resolved. The processes for cloud accreditation, Cloud audit assurance, etc. are required to be developed. Issues relating to Cloud Governance, data security and privacy for banks customers, etc. are not yet fully examined.

6. Keeping in view the limitations of the target banks, evolving nature of technology, open issues and security concerns, the Working Group recommends caution while adopting cloud computing solutions till all issues are understood and resolved. Where such innovative solutions are already adopted, the Working Group recommends suitable risk management measures as indicated in the report. In view of advantages of Cloud Computing, the Working Group recommends that support and Non financial services could be ideally explored as Cloud computing to gain more experience. Finally the Working Group recommends that there is need for more research and development in the area of Cloud governance and Audit, Cloud Management and Cloud Securing technology for which banking industry and software industry could take the initiative, so that regulatory authorities can make use of the same.

Chapter 1
Constitution of the working Group

1. **Introduction:**

Compared to commercial banks, the size, scale of operations, skill set availability, preparedness for computerisation of Urban Cooperative banks are not high. Yet, there is need for computerisation by adoption of Core Banking Solution (CBS) by these banks to derive greater reach and provide better services. In order to understand the options available, DG(AS) had meetings with two of the prominent CBS providing firms. EDs and CGMs-in-charge of DIT and UBD also participated in the meetings.

From the technology perspective following points emerged:

1. For a bank to adopt CBS on its own, it needs a minimum threshold limit in terms of number of branches, customers and number of transactions. It is possible for bigger Urban Cooperative Banks to adopt this approach.
2. For those UCBs, which cannot go for their own CBS, there are services models available. These service models are broadly termed as cloud services.
3. In cloud services, a service provider builds necessary resources in terms of hardware and software and allows individual banks to use them for a fee. The fee could depend on various factors like size, volume etc. As on date, two leading software solution providers are providing these services at a fixed cost.
4. The cloud technology is relatively new and is evolving. The issues relating to data confidentiality, security etc is yet to be completely established.
5. Further, there is excessive dependency by several banks on the service provider for all services. So drafting legal agreements etc. has to be fully considered.
6. Another dimension to the issue would be multiple service providers. Unless there are standards for both data and application, it would be extremely difficult to have systems that can talk to each other. More importantly for banks to move from one service provider to another.
7. There is lack on standardization in cloud computing terms of Security, Service Level Agreement, portability and interoperability, audit and accreditation.

Depending on size and financial status, UCBs can adopt either CBS of their own or draw services from service provider. DG desired that an approach paper for adoption of CBS/Cloud services may be prepared by DIT.

Accordingly, working group for exploring using Cloud Computing as option for small size Urban Cooperative Banks was set up with senior officers of DIT, UBD, DGBA, IT experts from the software industry and eminent Academicians in IT.

The composition of the Group is as under:

1.	Shri. A. K Hirve Chief General Manager Department of Information Technology Reserve Bank of India, Mumbai	Member Secretary
2.	Prof. G.Sivakumar Head, Computer Science and Engineering Department, Indian Institute of Technology, Powai	Member
3.	Prof. H. Krishnamurthy, Chief Research Scientist, Supercomputer Education and Research Centre Indian Institute of Science, Bangalore	Member
4.	Shri A. Udgata Chief General Manager-in-Charge Urban Banks Department Reserve Bank of India, Mumbai	Member
5.	Shri S. Ganeshkumar Chief General Manager Department of Government & Bank Account Reserve Bank of India, Mumbai	Member
6.	Tata Consultancy Services • Shri Satya Mishra • Shri Ujjwal mathur • Shri Jitendra Chivate	Member
7.	Infosys Limited Shri Deepak N. Hoshing Associate Vice President	Member

2. Terms of Reference:

a) To review the current level and use of IT infrastructure in UCBs

b) To ascertain the feasibility of using the service models available for CBS

c) To study the issues relating to data confidentiality, data security etc.

Chapter 2.
Methodology adopted by the Working Group

2.1 Methodology

The working group adopted following methodology for the study:

- **Review of the status of computerisation in the UCBs** - Implementation of recommendations of earlier working group: The RBI had set up a working group in December 19, 2007 for providing IT support to UCBs. The progress in implementation of the recommendation of this working group chaired by Shri R. Gandhi and the current status of implementation of core banking by UCBs was reviewed.
- **Review of Technology Trends for Cloud Computing** - The National Institute for Standards and Technology, U.S.A.(NIST) had undertaken research on cloud computing as an emerging technology trend. It had also taken initiative for cloud computing project by the US Government and published the reports for wider dissemination. The Information Systems Audit and Control Association (ISACA) had undertaken similar initiative to understand the Cloud Computing Governance as well as the Risk and Control aspects and Audit assurance framework for cloud based Information systems.
- **Review of Cloud like solutions Prevailing among UCBs** - The IT services providers had given presentation to the RBI Top management for the cloud services which they offered. During interaction with some of the leading UCBs, it was gathered that there has been industry trend among these banks to provide support and share the IT resources with each other. Some of the banks have been active in providing CBS as an Application Service Provider (ASP). Some of these banks and two software majors were requested to provide details and share their experiences in this regard.
- **Analysis** - The study team analysed the domestic and international trends in the context of models for core banking solutions proposed among small UCBs. The suggestions of the working group are based on the considerations of Security of banking application and customer data and identifying risks associated with Cloud computing for identifying the risk mitigation measures.

Scope :

The working group has looked only into the technology related aspects and has based its observations on the publically available information from the Standards setting organisations and the information obtained from the banks as well as software solution providers.

Chapter 3.
RBI initiative for UCBs and current status

3.1 The main recommendations of the Working Group on IT support to UCBs (Gandhi Committee) :

Considering the concentration of small UCBs, the lack of uniformity in the levels of computerization and inadequate awareness about the efficacy of computers in enhancing competitiveness, the minimum IT infrastructure was identified as:

a) Computerized front-end i.e. customer interface

b) Automatic backend accounting (through software)

c) Computerized MIS reporting; and

d) Automated regulatory reporting.

The working group had suggested Core Banking Solution (CBS) for adoption by the Urban banks. The models for acquiring the IT infrastructure were identified as

i) Application Service Provider (ASP) Model in respect of the small banks.

ii) Outright Purchase Model for banks which have a business of more than 100crores, CRAR of over 9% and have been profit making for the past 3 years.

3.2 Status of computerisation as on March 31, 2012

Table 1: State-wise no. of banks and no. of banks under CBS (March 31, 2012)

Sr. No.	State	No. of banks	No. of banks under CBS
1	Andhra Pradesh	104	14
2	Bihar	5	1
3	Delhi	15	8
4	Gujarat	237	55
5	Karnataka	265	14
6	Kerala	60	17
7	Maharashtra	529	124
8	Orissa	12	1
9	Rajasthan	39	16
10	Uttar Pradesh	75	7
11	West Bengal	47	1
Sub-Total		**1388**	**258**
12	Other States	230	9
Grand Total		**1618**	**267**

The Urban Cooperative banking sector is highly heterogeneous with concentration in a few states like Maharashtra and Gujarat. Further there are only limited numbers of

banks who have sizeable share of total banking business done by the UCBs. In terms of availability of IT infrastructure as well as business profile, these large UCBs are similar to old generation private sector banks. The UBD study revealed that around 42% banks are unit banks and further 13% banks have only two branches. Nearly 80% banks have less than five branches. The solution is intended for these banks. Further, these banks have a limited banking services provided to their customers. In terms of technical as well as banking skills these banks are extremely limited. Many of these banks have either limited or no profit and have been facing financial stress. The Reserve Bank has taken many initiatives in this sector for consolidation as well as for strengthening the banks as a regulatory requirement. However, the cooperative credit structure has evolved as a means to meet the financing requirements of people of small means and has a history of over hundred years. They serve an important purpose of financial inclusion. The proximity to their customers and ability to understand their requirements of small and micro enterprises has been a unique feature and as a result these are viewed as instruments of extending banking services to people with small means. Further, the UCB sector is also characterised by its dual control as state governments have control over the governance structure through Registrar of Cooperative societies and RBI having say over the banking services provided by these banks. The technology solution to be proposed is expected to help these banks to improve efficiency of their transaction processing capabilities, housekeeping and customer service as a means to meet the competitive pressure on these banks. In other words, the solution to be provided needs to provide a level playing field to these banks in terms of access to IT solutions.

Chapter 4:
Current Trends in Cloud Computing

4.1 Introduction to cloud Computing

4.1.1 Definition:

Cloud Computing has become ubiquitous concept (term / idea) in Information Technology arena and is widely agreed to be the key to future of IT. National Institute of Standards and Technology (NIST) has defined cloud computing as:

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

As per NIST definition, cloud computing needs to satisfy five essential characteristics, use one of the three service models and deploy using one of the four models as depicted in the following diagram:

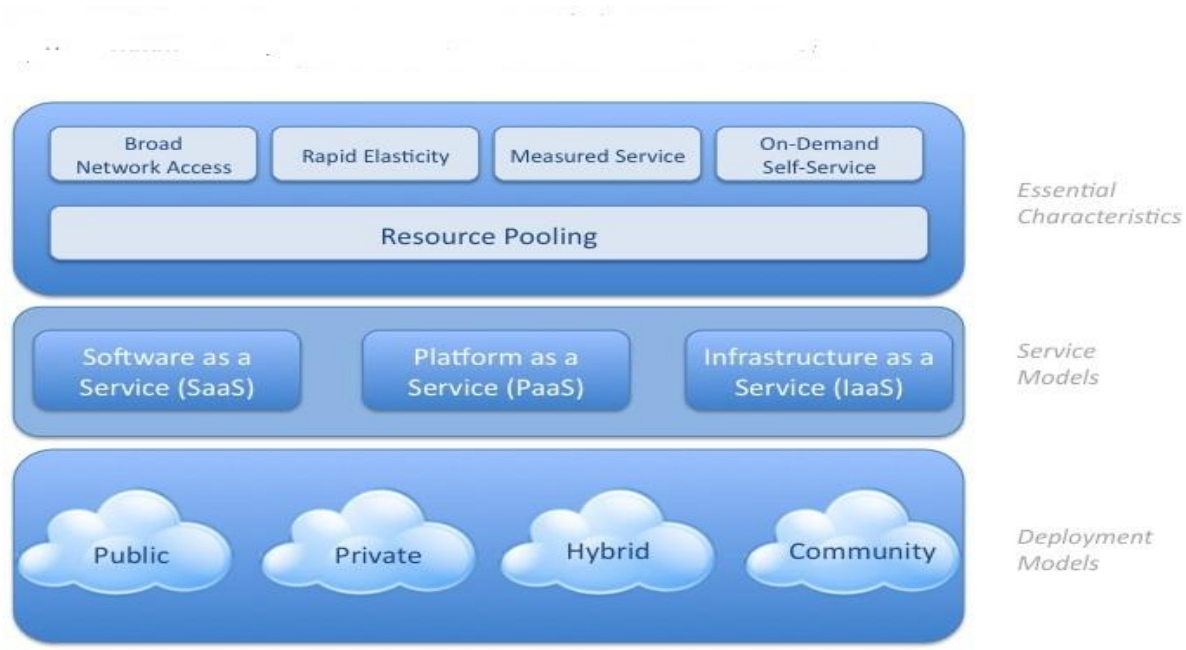


Fig 4.1 NIST visual model of Cloud Computing Definition

The five essential characteristic are (a) On demand self-service i.e. provisioning of additional computing facilities without human intervention (b) Broad network access i.e. accessibility from a variety of devices (c) Resource pooling i.e. sharing of

infrastructure like data centre, hardware, infrastructure software and application software across banks (d) Rapid Elasticity i.e. resources allocated to a bank can grow or shrink dynamically depending upon load and (e) Measured service i.e. pricing would be based on actual usage rather than cost of equipment.

Service models for would could be (a) Infrastructure as a Service (IaaS), which is typically used by IT managers / system administrators to commission additional machines on the cloud, typically to address temporary spikes in computing requirements (b) Platform as a Service (PaaS), where infrastructure on the cloud is used by application developers to develop applications and (c) Software as a Service (SaaS), where infrastructure on the cloud is used by end-users to use already developed applications. While all three models can be used by banks, "Software as a Service" which would be of relevance to cooperative banks considering that they have lean IT departments and model providers, higher level of abstraction which could help UCBs only on transaction processing while leaving details of HW, SW and Networking to the Service Provider.

Deployment options could be (a) private cloud, where the entire infrastructure would be meant for a single bank (b) public cloud, where infrastructure would be available to general public (c) community cloud, where infrastructure would be used by a group with common interests and (d) hybrid cloud, which would leverage infrastructure on more than one of the above deployment models. While all the above deployment models can be used by banks, this report would concentrate on understanding the model presently being used in the banking industry, in this case, urban cooperative banks.

Parties involved within various aspects of cloud deployment: Before we proceed further, we would like to depict roles and responsibilities of various parties involved in cloud deployment. This refers to conceptual reference model as described by NIST2.

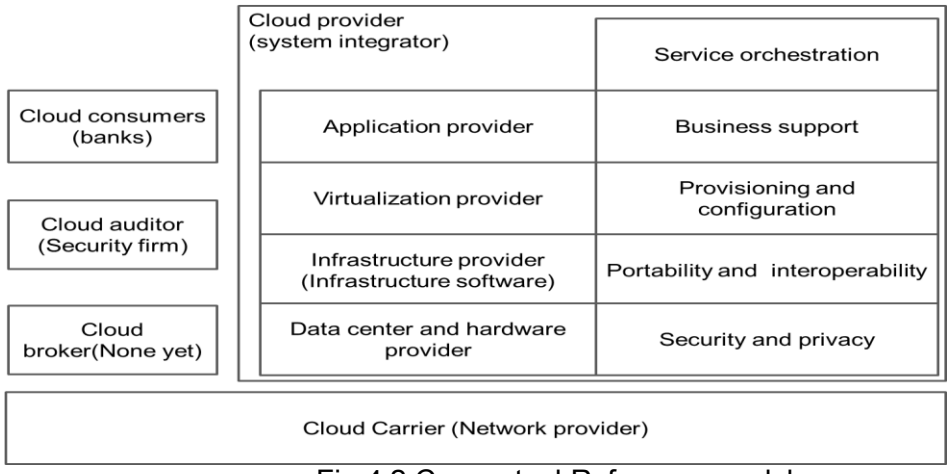


Fig 4.2 Conceptual Reference model

1. Cloud consumer: This could be a bank or any other consumer that would avail of services on the cloud.
2. Cloud provider: This would be a system integrator who would integrate offerings from multiple parties to provide a solution and sign contracts with cloud consumers. These parties would be (a) Data center and hardware provider (b) Infrastructure (software) providers (c) Virtualization (software) providers (d) Application providers and optionally (e) Network provider.
3. Cloud carrier: This would be the provider of network infrastructure to connect various bank branches to the data center.
4. Cloud auditor: This could be a reputed audit firm who can conduct an independent security, data privacy and performance audit of operational processes and deployment infrastructure. The scope of the audit could include banking aspects depending on the charter, which could be specified. It could also provide for inspection by the RBI.
5. Cloud broker: These parties would provide value added services using aggregation or arbitration on the top of business services provided by cloud providers. This is yet to evolve.

4.1.2 Essential characteristics:

On-demand self-service: Cloud allows consumer to unilaterally provision IT infrastructure in the cloud in terms of computing resources, network capacity, storage requirements, etc., on demand basis. This means that cloud provider should be able to provide additional computing capacity without human intervention e.g. addition of new branches or addition of new customers or accounts.

Broad network access: Cloud resources are accessible over the network through plethora of devices through standard mechanisms. Heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations) can be used to access cloud.

Resource pooling / Multi-tenancy: Cloud provider provides infrastructure, including data centre, air conditioning, power supply, hardware, infrastructure software,

storage, and network which can be shared between different consumers. There can be a logical separation between each consumer's computing resources and network using virtualization and VPNs or other techniques. Sample deployment diagram using virtualization is as shown in the figure below.

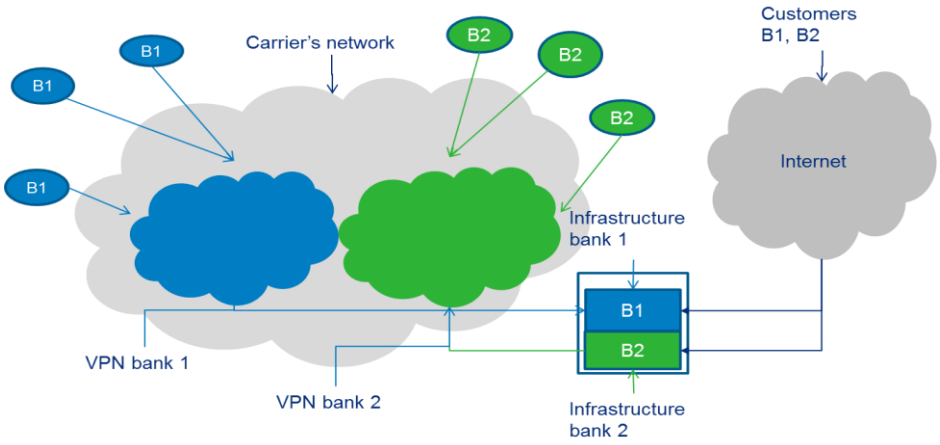


Fig 4.3Sample deployment diagram using virtualization

Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to scale rapidly outward and inward commensurate with demand. In the context of bank customers, the capabilities available can be appropriated in any quantity at any time.

Measured Service: Nature of Cloud service makes it possible to measure the usage of services/resources like storage, processing, bandwidth and active user accounts. Resource usage should be monitored, controlled, and reported; providing transparency for both the provider and consumer of the utilized service. In the context of banks, the Cloud provider should have reporting mechanism while billing.

4.1.3 Service Models:

Cloud Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Basically consumers are organizations and application providers for end users.

Control: As for the scope of control, service providers control most of the resources on the cloud and consumer has limited control of application related resources only.

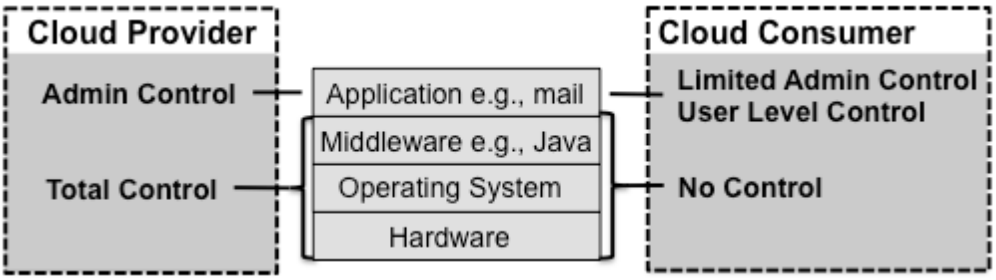


Fig 4.4 SaaS Provider/Consumer Scope of Control

Benefits: The key benefits of SaaS clouds are: very modest software tool footprint, efficient use of software licenses, centralized management and data, platform responsibilities managed by providers, and savings in up-front Costs.

Issues: But there are issues and concerns such as browser-based risks, network dependence, lack of Portability between SaaS, and isolation vs. efficiency (Security vs. Cost Tradeoffs)

Candidate applications: This model is useful for business logic (CBS, Customer Relationship Management, Inventory Management, Fund transfer), Collaboration (Email, Portal, etc.), Office Productivity (Word processors, spread sheet, presentations programs, etc), Software tools (Security scanning and analysis, compliance checking, etc).

Cloud Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. Here consumers are application developers, application testers, application deployers, application administrators, and application end users (Saas)

Control: As for the scope of control, service providers control most of the resources on the lower layer but less than as compared to SaaS cloud. Consumer enjoys slightly more control on application as well as middleware.

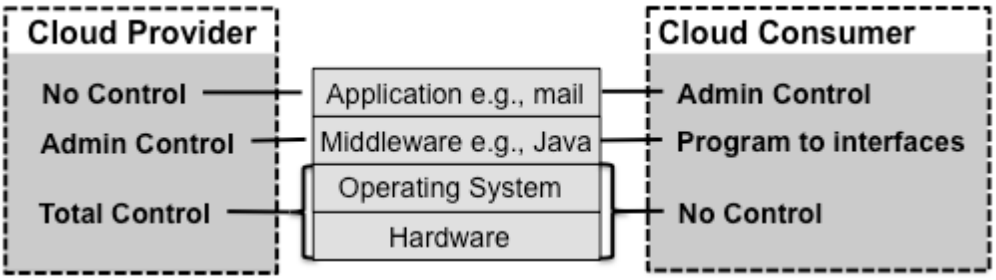


Fig 4.5 PaaS Component Stack and Scope of Control

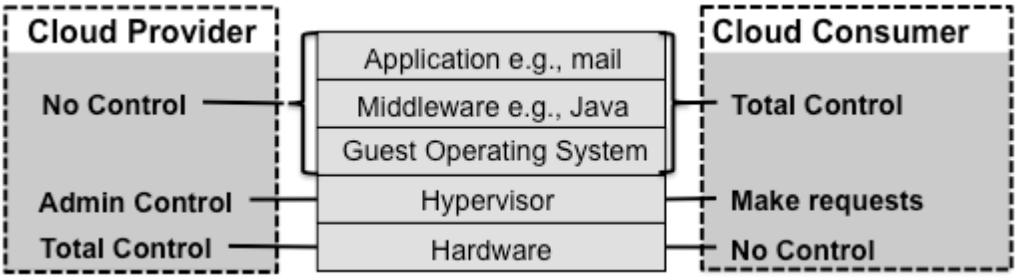
Benefits: PaaS clouds shares same benefits as SaaS namely very modest software tool footprint, efficient use of software licenses, centralized management and data, platform responsibilities managed by providers, and savings in up-front Costs. Apart from that it allows consumer a low cost option to develop and deploy the application on the cloud. This also helps to an extent overcome issue of lack of portability between service providers as consumer has control over application and data.

Issues: PaaS cloud has same issues as SaaS such as browser-based risks, network dependence, and isolation vs. efficiency (Security vs. Cost Tradeoffs). Apart from that portability across PaaS platform, have to provision more resources to honour time bound request and consumer has to maintain IT expertise to take care of application. In case it is provided by third party, then one more layer of complexity is added in service provider management for the consumer.

Candidate applications: This PaaS model is useful same set of applications as for SaaS viz. business logic (CBS, Customer Relationship Management, Inventory Management, Fund transfer), Collaboration (Email, Portal, etc.), Office Productivity (Word processors, spread sheet, presentations programs, etc), Software tools (Security scanning and analysis, compliance checking, etc).

Cloud Infrastructure as a Service (IaaS)*:* The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls). The consumer here is system administrators.

Control: As for the scope of control, service providers control most privileged lowest layer but less than as compared to PaaS cloud. Consumer enjoys much more control on application, middleware and OS.



IaaS Component Stack and Scope of Control

Benefits: IaaS clouds provide benefits in terms of savings in up-front Costs, allows full control of IT resources, flexible and efficient renting of resources, and its resolve the problems of portability and interoperability.

Issues: IaaS cloud has issues such as browser-based risks, network dependence, legacy application security issue, VM security issue in terms of missing security update, robustness of VM isolation, and data erase practices.

Candidate applications: This IaaS model is useful for system integrators or other service providers to develop test and deploy applications for end users/ organizations.

4.1.4 Deployment Models:

Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

***Public cloud*:** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)."

4.2 Reference Architecture for Cloud Computing

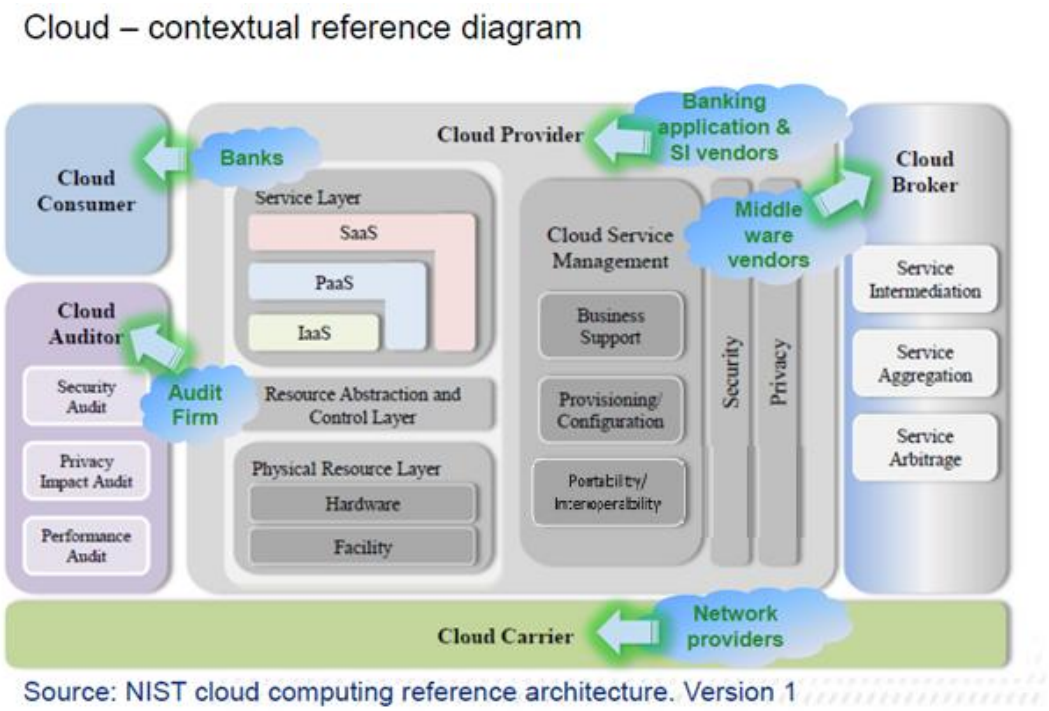


Fig 4.7 Cloud computing reference architecture

There are fundamental technical building blocks for cloud computing viz.

• SOA—A library of proven, functional software applets that can be connected to become a useful application

• Application programming interfaces (APIs)—Tags to direct applets about the Internet

• XML—Identifier tags attached to information (data, pages, pictures, files, fields, etc.) that allow them to be transported to any designated application located on the Internet

4.3 Open issues in cloud computing

Cloud services helps consumer to outsource the maintenance burden of servers and applications; scale systems up or down on demand; being able to access data from anywhere with a network connection; and the ability to replace occasional heavy capital expenditure (CAPEX) on IT with regular and predictable operational expenditure (OPEX). From a provider's perspective, cloud computing allows capital

expenses to be leveraged into positive revenue streams after initial investments are made.

Cloud computing is evolving technology and will contain flaws, experience failures, and experience security compromises. Different service aspects of Cloud are yet to be standardized like end-to-end security, Portability, Interoperability, Service level agreement, etc. There are some issues which are unique to it and some already exists.

There are challenges in adopting Cloud computing as can be seen from open issues such as Computing performance, Cloud reliability, Economic goals, compliance, and Information security, which are discussed below :

4.3.1 Computing Performance

Like any other form of computing on network, cloud computing face performance issue in terms of time take to process request over network, data synchronization, scalability of application and data management.

Latency is the time taken to process the application request over the network (round trip). Multiple components and hops are involved starting from the end user desktop (Interface card) to LAN, end user router, network cloud, perimeter of provider, LAN and ultimately the application. Clear cut demarcation and responsibility, network optimization tools, web acceleration technologies and application capabilities to an extent can assure certain level of acceptable performance.

Off-line Data Synchronization is critical for any network based application to take care of outages at network or consumer level. Technology adopted should be capable of taking care of version control and re-sync data.

Scalable programming to leverage the scalable computing and network resources will be needed. Applications need to be re-engineered to realize the full benefits of the new computing capacity, which will be available on demand.

Data storage management becomes critical issue as data, especially finance related, will be residing in the provider's cloud. Consumer should be able to scale data storage on demand basis, restrict physical location of the data at rest (database, tapes, etc) to handle issue of data sovereignty, ensure proper process for data purging and disposing of data storage hardware and administer access control over the data.

4.3.2 Cloud reliability

Reliability refers to the probability that a system will offer failure-free service for a specified period of time within the bounds of a specified environment. This issue is

more acute as services are availed from the cloud and are residing on provider's premises. Since cloud consists of multiple components, measuring reliability of individual component may be easier but difficult when taken together. Each component has specific reliability in given context and when all components taken together with their inter-dependencies, it will throw up more complications. The issue of reliability of the cloud depends upon the: Cloud provider outages (hardware, software and personnel's), connectivity to the subscribed services, and the consumer's personnel.

The provider's infrastructure {HVAC, IT components (hardware, software, network, security, etc.,) personnel's, physical security, etc.} is prone to outages due to hardware, software or man-made issues. The SLA should clearly reflect uptime and performance parameters and alternatives for contingency situations.

Network becomes critical component for any cloud based applications. It poses questions of availability on continuous basis, security risk for critical data in transmission, vulnerability to virus/worms/DOS attacks to name a few, physical cables cutting, natural disasters, etc. Network outages have to considered and contingency planning to be done for such events.

4.3.3 Economic goals

Cloud computing offers benefits to consumers in terms of converting their capex to opex and improve business agility by deploying and testing application and reaching to market in no time. But such benefits come with varied risks like risk of business continuity, SLA risk, portability and interoperability issues and disaster recovery.

Risk of business continuity is clearly visible where on-site resources can be run even if vendors have withdrawn or suspended the services. But in case of cloud, consumers are completely dependent upon service providers for running their IT services. In case of banks running their financial application like CBS, service provider suspension will bring complete halt to their whole business of banking.

Service Agreement is another area where consumers has to ensure that all aspects of cloud services are taken care of in terms of performance, outages, penalty, disaster recovery, portability, exit provision and data security, to name a few. Lack of standardization of SLA as well as difficulty in quantifying and measuring the terms of contract pose a greater risk to cloud consumer (UCBs).

Portability and Interoperability are related issues on cloud computing. Interoperability is like the successful communication between, or among systems, and portability is ability to use components or systems in multiple hardware or software environments. As for the portability, consumer should be able to migrate

from existing system to cloud or from one service provider to another or back to the consumer from cloud with least effort. Such portability demands standardisation at various interface level – network, application, middleware, etc. as well as at data format level. As for the interoperability consumer should be able to use other service providers cloud like during 'Cloud bursting' or a situation where cloud services of the provider are severely stressed.

Disaster recovery becomes more critical in cloud environment as it will impact number of consumers hosted in the service provider's cloud. Service provider should follow industry standard for DR site and setup, proper processes, and perform frequent DR drill.

4.3.4 Compliance

Consumers availing the cloud services are accountable to different stakeholders like end customers, regulators and other bodies for compliance. In cloud computing, the lack of visibility, jurisdiction and regulation issue, actual location of data, and support for forensics plays a critical role in compliance.

Consumer lacks visibility in cloud computing as how it operates and whether services are delivered in secured manner, end-to-end. Security event and information management at provider's end with information sharing with consumer will help to reduce lack of visibility.

Providers decide the physical cloud location on the basis of economic and other resources factors, whereas that may not meet the consumers compliance requirement like in case of data to be within national borders.

Consumers have to adhere to variety of regulations as stipulated by the respective industry regulators. Consumers, who are ultimately responsible for their data processed on provider's systems, will need to require assurances from providers that they are aiding in compliance of the appropriate regulations. This will require independent third party audit on regular interval basis to ensure that provider is meeting compliance requirements on continuous basis. Provider will have to agree for audit and investigative support and it can be made part of SLA. Consumers also need to know the legal jurisdiction and be able to get legal remedies for any failure on part of provider to meet contract terms.

As nothing is full proof, some incident or event is bound to happen. To take care of such security events and incidents, digital forensics has to be carried out. It should clearly delineate the roles and responsibilities between provider and consumer. Also mutually agreed process should be in place for incident and security breach handling and management.

4.3.5 Information security

Confidentiality and integrity of data with availability of data is the main crux of information security. Business critical information of consumer has to be monitored and protected at all level. As such, organizations employs various controls like Administrative controls for data operation, Physical control to protect storage media and facilities, and Technical control by employing Identity and Access Management, and by encrypting data in transit as well as at rest. In case of cloud, there are more complexity depending upon the way cloud is implemented, the attack surface of cloud, types of attackers, system complexity, expertise level of cloud administrators, to name a few.

Data has to be protected during transit and at rest by encrypting with sufficient long key length and proper key management. Data privacy has to be maintained through legal and technical channel. More so; in multi-tenancy environment where multiple customers access, application and data resideing in same physical boxes. Access segregation, application segregation and more so data segregation has to be done using advance technology and clear cut process and guidelines to be laid down for the same. Privileged access to data has to monitored and controlled.

Even consumers has to ensure that interface (thin or thick client) use by them to access the cloud services is secured, updated with latest patch and well protected.

4.4 Saas model and issues in implementation

Cloud Software as a Service (SaaS): SaaS as introduced in 4.1.3 prima facie seems to more suitable model for cloud computing especially for smaller banks. The applications are accessible from multiple devices. The consumer does not manage or control the underlying cloud infrastructure.

Benefits: The key benefits of SaaS clouds are: very modest software tool footprint, efficient use of software licenses, centralized management and data, platform responsibilities managed by providers, and savings in up-front Costs.

i) Very Modest Software Tool Footprint: As browsers that are capable of efficiently displaying interactive content have become ubiquitous, SaaS application deployment has become increasingly convenient and efficient with little or no client-side software required. Several factors contribute to this value proposition:

- Unlike shrink-wrapped software applications, SaaS applications can be accessed without waiting for complex installation procedures.

- Because SaaS applications have very small footprints on client computers, risk of configuration interference between applications on client computers is reduced.
- Distribution costs for the software are reduced. Lower distribution costs allow for economical development and deployment of software features even if they appeal to only a small portion of consumers.

ii) Efficient Use of Software Licenses: License management overheads can be dramatically reduced using SaaS. Consumers can employ a single license on multiple computers at different times instead of purchasing extra licenses for separate computers that may not be used and thus over-provisioning the license. Additionally, traditional license management protocols and license servers are not needed to protect the intellectual property of application developers because the software runs in the provider's infrastructure and can be directly metered and billed.

iii) Centralized Management and Data: The SaaS service model implies that the majority of the data managed by an application resides on the servers of the cloud provider. The provider may store this data in a decentralized manner for redundancy and reliability, but it is centralized from the point of view of consumers. This logical centralization of data has important implications for consumers. One implication is that, the SaaS provider can supply professional management of the data, including for example, compliance checking, security scanning, backup, and disaster recovery. When these services are provided away from the consumer's premises in public and outsourced scenarios, SaaS management of data gives consumers protection against the possibility of a single catastrophe destroying both the consumer's facility and data. This benefit, however, is contingent upon the SaaS provider protecting its facilities from catastrophic attack or other undesirable events. The “on demand” network access of SaaS applications also relieves consumers from the need to carry their data with them in some settings, thus potentially reducing risks from loss or theft. When supported by the application's logic, remote data management also facilitates sharing among other consumers.

iv) Platform Responsibilities *Managed by Providers:* Generally, for outsourced or public SaaS clouds, consumers need not become involved with the management of a provider's infrastructure. For example, consumers need not be distracted by which operating system, hardware devices or configuration choices, or software library versions underlie a SaaS application. In particular, providers have

responsibility for operational issues such as backups, system maintenance, security patches, power management, hardware refresh, physical plant security, etc. Providers also have an obligation to field services that guard against known exploits at the application level. Further, consumers are not required to maintain on premises IT support to perform these tasks, with an exception that on premises IT support is still necessary to connect consumer browsers securely to the network. Because SaaS providers implement new application features and provide the server side hardware that runs them, SaaS providers also have advantages in managing the introduction of new features while mitigating the need for consumers to upgrade their hardware systems to use the new features.

v) Savings in Up-front Costs: Outsourced and public SaaS clouds allow a consumer to begin using an application without the up-front costs of equipment acquisition, but potentially with a recurring usage fee. Additionally, cloud providers should be able to provision their hardware, power, and other computing resources at scale and more efficiently than individual consumers, which may reduce ongoing costs to consumers. This provides a basis for cost savings to consumers.

Issues and concerns: But there are issues and concerns such as browser-based risks, network dependence, lack of Portability between SaaS, and isolation vs. efficiency (Security vs. Cost Tradeoffs)

i) *Browser-based Risks and Risk Remediation:* Although browsers encrypt their communications with cloud providers, subtle disclosures of information are still possible. For example, the very presence or absence of message traffic, or the sizes of messages sent, or the originating locations may leak information that is indirect but still of importance to some consumers. Additionally, even strong cryptography can be weakened by implementation mistakes; a common mistake is to generate keys or passwords in a manner that reduces their strength, thus making the cryptography vulnerable to brute-force guessing attacks. Furthermore, man-in-the-middle attacks on the cryptographic protocols used by browsers [Mar09] can allow an attacker to hijack a consumer's cloud resources. By relying on a consumer's browser for software application interfaces, the SaaS approach also raises a risk that, if a consumer visits a malicious Web site and the browser becomes contaminated, subsequent access to a SaaS application might compromise the consumer's data. Another risk is that data from different SaaS applications might be inadvertently mixed on consumer systems within consumer Web browsers.

One work-around to this issue is for consumers to use multiple browsers and to dedicate specific browsers to important SaaS applications and not to perform general-purpose Web surfing that may expose them to attack. Another work-around is for consumers to use a virtual desktop when connecting to cloud-hosted applications, which provides a secure, fully functional work platform that is governed by strict policies for limiting what can or cannot be accessed elsewhere, while connected to a cloud.

ii) *Network Dependence:* The availability of a SaaS application depends on a reliable and continuously available network. In the public SaaS cloud scenario, the network's reliability cannot be guaranteed either by the cloud consumer or by the cloud provider because the Internet is not under the control of either one. In outsourced private or community SaaS scenarios, network security and reliability can be achieved using dedicated, protected communications links, but at a cost. Although a SaaS application may include a "disconnected mode" for continued processing during network outages, the fundamental organization of SaaS, with application logic implemented on the cloud provider's servers, implies that the actual functionality of the application will be dependent on its ability to access a reliable network.

iii) *Lack of Portability between SaaS Clouds:* Portability in SaaS is a concern for transitioning workloads from one SaaS cloud to another. Formats for exporting and importing data may not be fully compatible among SaaS clouds. Customized workflow and business rules, user interface and application settings, support scripts, data extensions, and add-ons developed over time can also be provider specific and not easily transferable.

iv) *Isolation vs. Efficiency (Security vs. Cost Tradeoffs):* There exist a trade-off between isolation and efficiency as well as security vs cost depending upon how application software is executed by a SaaS provider.

Candidate applications: This model is useful for business logic, Collaboration , Office Productivity, and Software tools:

- **Business logic.** Applications in this area connect businesses with their suppliers, employees, investors, and customers. Examples include invoicing, funds transfer, inventory management, and customer relationship management

- **Collaboration.** Applications in this area help teams of people work together, either within or between organizations. Examples include calendar systems, email, screen sharing, collaborative document authoring, conference management, and online gaming.
- **Office productivity.** Applications in this area implement the applications that typify office environments such as word processors, spreadsheet programs, presentation programs, and database programs. In their SaaS incarnations, these applications often offer collaboration features missing from traditional office productivity applications.
- **Software tools.** Applications in this area solve security or compatibility problems and support new software development. Examples include format conversion tools, security scanning and analysis, compliance checking, and Web development

Recommendations: The following are additional recommendations for SaaS systems:

- **Data Protection.** Analyze the SaaS provider's data protection mechanisms, data location configuration and database organization/transaction processing technologies, and assess whether they will meet the confidentiality, compliance, integrity and availability needs of the organization that will be using the subscribed SaaS application.
- **Client Device/Application Protection.** Protect the cloud consumer's client device (e.g., a computer running a Web browser) so as to control the exposure to attacks.
- **Encryption.** Require that strong encryption using a robust algorithm with keys of required strength be used for Web sessions whenever the subscribed SaaS application requires the confidentiality of application interaction and data transfers. Also require that the same diligence be applied to stored data. One must apply cryptographic algorithms for encryption and digital signature. Understand how cryptographic keys are managed and who has access to them. Ensure that cryptographic keys are adequately protected.
- **Secure Data Deletion.** Require that cloud providers offer a mechanism for reliably deleting data on a consumer's request.

4.5 Security issues in cloud computing

As discussed earlier, cloud computing is evolving technology and could be expected to contain flaws, experience failures, and security compromises. There are some issues which are unique to Cloud Computing. NIST has identified Process oriented and Technical oriented security features to rectify or mitigate the known security issues in cloud computing.

4.5.1 Process-oriented security requirements

Process oriented security covers Security controls, Cloud Audit & assurance, log management, Cloud Certification and Accreditation, Cloud privacy guidelines, Clarity on cloud actors security roles & responsibilities, Trustworthiness of cloud operators, BCP and DR of cloud services, and Continuous Monitoring capabilities.

- Security controls define minimum recommended management, operational, and technical controls for information systems based on impact categories. Consumers must ensure that the Service Level Agreements (SLAs) legally binds the Cloud Provider, Broker or Carrier to implement all necessary security controls deemed appropriate and applicable.
- Cloud Audit & assurance security requirement identifies the needs to gain assurance that important events are monitored; sensitive/private audit logs are appropriately protected; integrity of audit data used for initial or continuous auditing purposes is protected; and audit data interchange incompatibility is resolved. Audit data to be encrypted and stored in the media like Write Once and Read Many times (WORM). Also SIEM (Security Information and Event Management) for continuous monitoring has to be followed. SLA should delineate the task of monitoring, auditing and information sharing. It is more complex in case of multi-tenancy.
- Cloud Certification and Accreditation requirement addresses the need to certify and accredit cloud solutions with confidence. The risk management process changes the traditional focus of Certification and Accreditation (C&A) from a static, procedural activity to an increasingly dynamic approach that provides the capability for more effective management of information system-related security risks in a highly diverse environment of complex and sophisticated cyber threats, ever-increasing system vulnerabilities, and rapidly changing missions.
- Cloud privacy guidelines requirement addresses the need to build confidence in cloud solutions that provide privacy of data and personally identifiable information (PII) protection. Consumer has to ensure that SLA and/or contracts require cloud service providers to adhere to existing guidance regarding privacy and PII

information. Ultimately, it is the system owner and approving authority that are responsible for the proper handling of such data.

- Clarity on cloud actors security roles & responsibilities is required for clearly delineating the roles and responsibilities among cloud actors (e.g., cloud consumer and cloud service provider) for the implementation of required security controls. The actor most able to observe and configure specific components of a cloud implementation is in the best place to implement a relevant control.
- Trustworthiness of cloud operators needs to be established to ensure that individuals with physical and logical access to consumer data are properly vetted and screened periodically to ensure trustworthiness. This is one of the major issues for consumer's reluctance to adopt cloud services and solutions.
- BCP and DR of cloud services is must in the cloud environment where multiple consumers are hosting their critical and not-so critical applications. Consumer in service industry will be adversely impacted with unavailability of cloud for their services and solutions. Redundant architecture for high availability coupled with DR site is must for cloud. Well defined policies and procedures need to be defined and implemented clearly stating ownership, data sensitivity, cloud service and deployment models, roles and responsibilities, indicating Recovery Point Objective (RPO) and Recovery Time Objective (RTO), etc.
- Technical continuous monitoring capabilities are necessary to support cloud environments. For cloud providers, it is critical that they be able to gain situational awareness of their cloud environment and to provide evidence to their customers that the cloud infrastructure is secure. It also may be important to provide customers feedback on the security of their use of the cloud.

4.5.2 Technical-oriented security requirements

Technical-oriented security requirements cover Visibility for consumers, Control for consumer, Data Security, Risk of Account Compromise, Identity Credentials and Access Monitoring and Authorization, Multi-Tenancy Risks and Concerns, Cloud based Denial of Service, and Incident Response.

- Visibility for consumer's requirement discusses the fact that cloud consumers have very limited visibility into the provider's security measures and the related incident alert and audit information with respect to cloud resources and customer's data and applications. Consumers to be able to observe their workload and monitor their security, privacy, system health and general status. Further to be able to instruct provider to share such data is important as

consumer is ultimately responsible for security and privacy of their information and has to comply with regulatory requirements. Thus provider does not need desperate tools but need unified tools to monitor and manage entire cloud.

- Control for consumer is very limited over security policies enforced by cloud providers on their behalf. There is also very little automation available to help customers to implement technical controls (policies) across their cloud applications. Question arises how consumer will monitor and instruct providers on security aspects. Mutually they need to define and enforce security policies including Identity and access management.
- Data Security is must as loss of confidentiality, integrity, or availability of consumer's data can impose a wide variety of impacts. Cloud consumers need to understand the extent of the data protection that a cloud offers so that they can make rational risk-based decisions availing cloud services. Data in transit, data at rest and data in computation has to be protected. Data life cycle management policy to be defined and implemented. Same can be audited by third party to ensure compliance by provider.
- Risk of Account Compromise is more in cloud as it is network resource. More so when network is public i.e. Internet where multiple threats exists in terms of phishing, pharming and spyware, whose purpose is to steal usernames and passwords (credentials). Mitigations such as strong authentication, encrypted credentials, and secure APIs/interfaces have been used to protect user accounts from hijack. But it has to be coupled with user's education to follow security practices like not to click phishing email.
- Identity Credentials and Access Monitoring and Authorization is critical for cloud security as unauthorized access to sensitive information in clouds is a major security concern for both customers and providers. Due to the broad network access characteristic of cloud computing, remote authentication of individual user is a common practice, and it presents a technical challenge to establish the needed level of confidence in user identity commensurate with information sensitivity. The identity credential and access management should be effective and scalable.
- Multi-Tenancy Risks and Concerns are valid as cloud is based on providing cloud services and solution on shared basis. Different tenants use services on the same cloud simultaneously. Although many network services and programs have simultaneously supported multiple tenants in the past, cloud computing elevates this concern because the resource sharing is pervasive, exposes many possibly

vulnerable interfaces, and potentially occurs at a very large scale. Segregation at network, application and data storage level has to be ensured to mitigate multi-tenancy risk.

- Cloud based Denial of Service cannot be avoided even with clauses in SLAs that imply high availability and minimal downtimes for subscribers. Service or utility outages remain possible due to man-made causes (e.g., malicious attacks or inadvertent administrator errors) or natural causes (e.g., floods, tornados, etc.). DoS existed earlier but cloud computing risk is more due to more attach surface. Due to multi-tenancy, DoS attacks may be launched by insiders through shared resources, for example, via side channel attacks. Malicious users can initiate distributed DoS using the vast resources of cloud to the level of severity never seen before. One prevalent solution to withstand DoS attacks is to provide diversity and redundancy in networking and data processing and to use multiple cloud service providers. Another traditional solution is to use modern network devices that recognize DoS signatures and prevent DoS traffic. However, the separation and isolation mechanisms in cloud to protect against inside DoS attacks are still evolving and vendor-dependent. Finally, cloud computing depends on strong identity credential and access management (ICAM) to keep malicious users at bay.
- Incident Response and computer forensics in a cloud environment require fundamentally different tools, techniques, and training to assess a situation and capture appropriate evidence accurately when conducting an incident response that follows standard response guidelines. The response plan should address the possibility that incidents, including privacy breaches and classified spills, may impact the cloud and shared cloud customers. Cloud providers are required to develop and provide a documented incident response plan, as a deliverable

4.6 Audit issues in cloud computing

Audit plays much more critical role in cloud environment due to multiple consumers availing with critical and not-so critical service and solution and can have systemic wide implications, if consumers are from systemically important infrastructure services like finance and banking, power, etc. Audit can play more proactive role to ensure sustainability of cloud services with minimum outages and security breach. As a first step, enterprises need to clear about availing cloud services and solutions. The Information Systems Audit & Control Association (ISACA) has undertaken extensive research on Audit Assurance issues and IT Governance issues specific to Cloud Computing which are discussed below:

4.6.1 ISACA Guiding principles for cloud computing

ISACA has provided six guiding principles for cloud computing adoption and use. It has stated that it is too early in the life cycle of cloud computing to propose strict rules for the adoption and use of cloud infrastructures, platforms or software services. However; ISACA feels that principles that provide prudent boundaries of behaviour or describe a basic quality of trust or value applicable to cloud computing will help support decision making that will, in turn, reduce pressures and control risk. The six guiding principles for adopting and using the cloud are Enablement, Cost Benefit, Enterprise Risk, Capability, Accountability and Trust:

1. **Enablement:** To plan strategically for cloud adoption and use, enterprises need to:

- Treat cloud computing adoption and use as a strategic business decision.
- Make informed decisions, considering both business and operational needs and the benefits that can be provided by cloud computing.
- Communicate cloud computing arrangements and agreements to internal parties to ensure proper alignment and consistent oversight.
- Periodically review organizational strategies and the contribution of IT to ensure that cloud initiatives maximize Value delivery, Risk management and Resource utilization.

2. **Cost benefit:** To properly evaluate the costs and benefits of cloud computing, enterprises need to:

- Clearly document expected benefits in terms of rapid resource provisioning, scalability, capacity, continuity and the cost reductions that the cloud services offer.
- Define the true life-cycle cost of IT services provided internally or through a provider to have a basis for comparing expected and received value.
- Balance cost with functionality, resilience, resource utilization and business value.
- Look beyond cost savings by considering the full benefits of what cloud services and support can provide.
- Periodically evaluate performance against expectations

3. **Enterprise risk:** To understand the risk implications of cloud computing, enterprises need to:

- Consider the privacy implications of comingling data within the virtualized computing environment.
- Evaluate privacy requirements and legal restrictions, considering client needs as well as provider restrictions and capabilities.
- Determine the accountability addressed in SLAs, the ability to monitor performance and available remedies
- Understand current risk identification and management practices and how they need to be adapted to address risk management for cloud computing.
- Integrate scenario analysis into business risk management decision making.
- Consider exit strategy and the implications of not being able to render data as enterprise applications are sunset or unavailable.

4. Capability: To leverage both internal and cloud provider resources effectively, enterprises need to:

- Understand the human and technical resource capabilities that exist in the current infrastructure and how a cloud strategy will impact the need for these or other resources.
- Define the capabilities that a cloud provider will make available as well as constraints on these resources, including periods of unavailability or priority of use.
- Consider emergency situations and resource requirements necessary to determine causes, stabilize the environment, protect sensitive and private information, and restore service levels.
- Determine how policies, practices and processes currently support the use of technology; how transitioning to a cloud solution will require policy, practice and process changes; and the impact these changes will have on capabilities.
- Ensure that service providers can demonstrate that personnel understand information security requirements and are capable of discharging their protection responsibilities.
- Ensure that internal staff has the skill and expertise to coordinate activities with cloud providers and that they are engaged in cloud service acquisition and ongoing management.
- Ensure that effective channels of communication are provided with provider management and key specialists, particularly for problem identification and resolution.

5. Accountability: To ensure that responsibilities are clearly understood and individuals and groups can be held accountable, enterprises need to:

- Understand how traditional responsibilities are assigned and implemented within the existing organizational structure and as a part of policies and practices to determine how these are addressed within cloud solutions.
- Determine how responsibilities between tenant and provider organizations for cloud solutions are assigned and how communications between accountable individuals and groups will be facilitated.
- Ensure that processes and procedures provide a mechanism to ensure that responsibilities are accepted and accountabilities are clearly assigned.
- Maintain within the governance structure a means of reviewing performance and enforcing accountabilities. Consider the risk to the enterprise as part of the enterprise risk management program, the impact of potential lapses in assigned responsibilities, or the impact of not being able to assign accountabilities.

6. Trust: To ensure that business processes that depend on cloud computing can be trusted, enterprises need to:

- Clearly define confidentiality, integrity and availability requirements for information and business processes.
- Understand how reliance on cloud computing solutions may impact trust requirements.
- Structure the efforts of security, risk management and assurance professionals within both tenant and provider organizations to ensure that trust requirements are known and satisfied.
- Monitor changes in business use of cloud computing, vulnerabilities associated with cloud solutions, and implementations across tenant and supplier environments to ensure that threats to trust can be identified and resolved.
- Ensure that cloud infrastructure, platform and software service providers understand the importance of trust and create solutions that can be trusted.
- Provide ongoing assurance that information and information systems can be trusted.

4.6.2 Control objectives for cloud computing by ISACA

Control objectives sets good practices for the ends, by providing enterprises with the structure they require to measure, monitor and optimise the realisation of business

value from investment in IT / cloud. COBIT addresses IT / cloud risk and controls throughout an entire program life cycle. Reflecting actual program implementations, these risk controls are interrelated. the Control objectives framework included following four domains which in turn contain processor.

• **Plan and Organize (PO)**—Provides direction to solution delivery (Acquire and Implement) and service delivery (Deliver and Support). Which are other two domains.

• **Monitor and Evaluate (ME)—**Monitors all processes to ensure that the direction provided is followed. Effective IT performance management requires a monitoring process. This process includes defining relevant performance indicators, systematic and timely reporting of performance, and prompt acting upon deviations. Monitoring is needed to make sure that the right things are done and are in line with the set directions and policies. The COBIT framework is a generic framework for all IT infrastructure and as Cloud Computing emerged, the framework has been suitably adjusted to the features of Cloud computing.

4.6.3 Cloud governance - ISACA

ISACA defines IT Governance as the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved and ascertaining that risks are managed appropriately. The Cloud Computing is accelerating and mandating the transition and, therefore, Cloud Governance is necessary. When enterprises decide to utilize cloud services for some or all IT services, business processes are impacted, which makes governance more critical than ever. In such cases, enterprises should:

• Effectively manage increasing risk, including security, compliance, projects and partners

• Ensure continuity of critical business processes that now extend beyond the data center

• Communicate clear enterprise objectives internally and to third parties

• Adapt easily. Flexibility, scalability and services are changed in the cloud, enabling the enterprise and business practices to adjust to create new opportunities and reduce cost.

• Facilitate continuity of IT knowledge, which is essential to sustain and grow the business

• Handle a myriad of regulations

For enterprises to gain benefit from the use of cloud computing, a clear governance strategy and management plan needs to be developed. The strategy should set the direction and objectives for cloud computing within the enterprise, and the

management plan should execute the achievement of the objectives. Enterprise governance of cloud projects requires acknowledgment of regulatory compliance requirements at both where the data are sourced and where the data are stored. New legal issues are already arising relative to the cloud. Detailed due diligence (know your provider, right to audit, assured continuity, security policy and process transparency), an understanding of expected cloud client responsibilities, and review and negotiation of candidate service provider SLAs and contracts are necessary while opting for Cloud Solutions.

4.6.4 Audit charter for Cloud environment - ISACA

Objective and Scope of Audit

Objective—The cloud computing audit/assurance review will:

• Provide stakeholders with an assessment of the effectiveness of the cloud computing service provider's internal controls and security

• Identify internal control deficiencies within the customer organization and its interface with the service provider

• Provide audit stakeholders with an assessment of the quality of and their ability to rely on the service provider's attestations regarding internal controls

The cloud computing audit/assurance review is not designed to replace or focus on audits that provide assurance of specific application processes and excludes assurance of an application's functionality and suitability.

Scope—The review will focus on:

• The governance affecting cloud computing

• The contractual compliance between the service provider and customer

• Control issues specific to cloud computing

• Identity management (if the organization's identity management system is integrated with the cloud computing system)

• Security incident management (to interface with and manage cloud computing incidents)

• Network perimeter security (as an access point to the Internet)

• Systems development (in which the cloud is part of the application infrastructure)

• Project management

• IT risk management

• Data management (for data transmitted and stored on cloud systems)

• Vulnerability management

***Minimum Audit Skills*:** As per ISACA guidelines, Cloud computing incorporates many IT processes. Since the focus is on information governance, IT management, network, data, contingency and encryption controls, the audit and assurance professionals should have the requisite knowledge of these issues. In addition, proficiency in risk assessment, information security components of IT architecture, risk management, and the threats and vulnerabilities of cloud computing and Internet-based data processing is also required.

Implications for the proposed solution for UCB

The review of available professional literature indicates that Cloud Computing is an emerging discipline in IT based services. The standards in various areas are still emerging and only a broad framework is suggested. The cloud model has different roles as cloud provider, cloud carrier, cloud consumer and the cloud auditor. The role of Cloud auditor is important for providing assurance on many issues. Although the skill sets at the end users could be lower, the knowledge and skills for designing, implementing as well as for evaluating and for auditing Cloud Computing environment are complex and demanding.

Chapter 5
IT based Solutions used among Urban Cooperative Banks

Two major Software solution providers have provided their core banking solutions to UCBs, RRBs and District cooperative banks through their own Data Centres. Some of the major Urban Cooperative banks have also been providing IT support to the small Urban cooperative banks and having collaborative arrangements among themselves for sharing common IT infrastructures such as Data Centres and ATM networks. The working group requested six cooperative banks located in and around Mumbai Region and two leading software companies regarding IT support services provided by them to the UCBs. The solution providers were also requested to share their experience and suggestions on how IT support extended to small size UCBs.

5.1 IT Solutions provided by the Urban Cooperative Banks:

The responses from six UCBs in Maharashtra region, who shared information with their IT support services, are tabulated in the annexure in this chapter. The banks have indicated their collaboration and support as under:

Consultancy and training services:

- Drawing Technology roadmap for the banks.
- Drawing the Security Policy and Trainings
- Business Process Reengineering
- Advisory Services for establishing Bank Data Centre
- Network & MPLS evaluation for Bank
- IT training, etc.

Services such as Infrastructure as a Service:

- Sharing Primary Data Centre resources in terms of computing facilities, network, databases and storage etc.
- Acting as DR site for other cooperative banks
- Sharing of ATM network and payment facilities

Services such as Software as a Service / ASP:

- Sharing *CBS* solution with other banks on per branch / month fees.

Product Offerings: Developing and selling the products which are used in the banks for :

- Anti-Money Laundering Application
- Audit Compliance
- Business Intelligence and Reporting, etc.

Access to Electronic Payment system

- Sub membership for RTGS / NFS to other smaller banks.

It was observed that these banks which were based in western Maharashtra were providing solutions and services to urban banks located in states like J &K, West Bengal, Gujarat, Madhya Pradesh, Tamil Nadu, Karnataka, etc. Similarly the Software Solutions providers had then providing support to banks located across India. Thus, the geographical proximity or separation was not a either constraining or contributory factor and cloud services were geography neutral due to availability of good telecommunication network.

5.2 IT Solutions presently provided by Solution providers

ASP model provided by Software Developers

Cloud type services are provided by many software companies. Full details could not be ascertained but as per the responses received one of the solution providers has been providing core banking solution to around 53 banks and last year it had around 5800 branches using its ASP model. The software company has been pursuing with many more banks and has been awarded contract for ASP model for about 70 Cooperative banks in Rural credit structure. During the discussion it was informed that two major software companies in India were partners in this regard and this would be extended across India.

5.2.1 Cloud Services: The cloud model of the company comprises services which can be classified as IaaS and as SaaS. These include shared hardware and software, data centre and DR site, network services, Data backup and replication, etc.

- systems integration –requirement analysis to solution
- Network management from identifying service provider to ensuring uptime
- Data centre and Disaster Recovery sites
- Providing core banking solution on the cloud and software maintenance
- Product Customisation and change requests management
- Customer Relationship Management.

5.2.2 Cloud security features :The security features mentioned by the cloud providers are :

- Authentication at DNS server and at firewall,
- Virtual OS level clustering

- Port level authentication
- Database level authentication

5.2.3 Technical capabilities: The Cloud like service provider has a dedicated project team comprising project managers and other IT professionals to ensure monitoring of SLA.

In terms of geographic spread as well as banking business volume handled by cloud solutions, the cloud provider has significantly large share and it has provided link to ATM networks for its cloud solutions. Wherever the leased line telecom network is not available, access is provided over satellite network. Thus the service provider can provide facilities even to executors.

5.3 Initiatives taken by Industry Association - NAFCUB:

The NAFCUB which is an Industry association of UCBs has identified CBS six vendors all over the country through a bidding process. The NAFCUB has approved ASP model for Core banking for UCBs at a monthly rental of Rs 12,900 per branch per month. NAFCUB has stated that about 350 banks have migrated to CBS so far.

5.4 Constraints faced by small UCBs in IT adoption – views of solution providers :

The UCB sector is highly heterogeneous with around 42% of UCBs being unit banks, about 13 % having 2 branches, and about 20 % having 3 to 5 branches. Only 25 % of the UCBs have more than 5 branches. In view of their small size and geographical locations, small UCBs face issues of financial affordability, lack of IT awareness, technical as well as vendor management skill, procedural guidelines, language barrier, etc. A few of the IT related issues as stated by the solution providers are as follows:

- Security of the data and its ownership was the main concern raised by the small UCBs in case of cloud solutions.
- Legacy Data conversion poses significant challenge while migrating to CBS.
- Reluctance to IT associated process changes or reengineering.
- Lack of IT skills at operating level
- Decision makers inability of to negotiate with different vendors and technology.
- Difficulties faced in obtaining Network connectivity.
- Lack of awareness for Electronic Data Security among the employer.

- Language barrier while dealing with English interface in solutions

It was also mentioned that these banks face difficulties in procurement of branch level hardware due to procedural delays, difficulties in identifying reliable vendors. Similarly, preference to the individual or local level software providers who lack adequate resources and strength had often posed problem to many banks in the long run.

5.5 Suggestions proposed by the solution providers(UCBs and Industry):

5.4.1 Suggestions from UCB service providers: As per the feedback from leading UCBs, the UCBs will derive multiple benefits from business and technological perspective, if they go for the cloud based solution (SaaS / ASP model) for banking related applications, CBS being one of the main application. This will ensure Technical inclusion of weak UCBs and improve process of Financial Inclusion. The benefits that will accrue to UCBs will be:

- Increased Operational Efficiency and Anywhere banking
- Integration with ATM network, RBI CBS, NEFT, RTGS, government treasury, etc.
- Better compliance with regulatory provisions
- Better risk & Asset Management
- Reduced time to Market for New products
- Reduced Reconciliation Overhead and reduced transaction cost
- Focus on core banking business
- Moving from Capital Expenditure to Operational Expenditure.
- Managing without specialized IT skill set
- Freedom from Technological Obsolescence.

5.4.2 Views / Suggestions by the Software solution providers :

One of the suggestions received was related to **the**consortium of UCBs and software company for cloud computing solution. The input provided by a software major mentions various cloud based banking services being provided and used in banks besides core banking as share accounting, HR and Payroll management, funds and investments, credit application processing and tracking, liquidity forecast, etc. In the opinion of the software major, infrastructure facilities such as channels like switches for ATM or IVR could also be deployed on cloud. The proposal has a cautionary suggestion which mentions a need for strong audit, clarity for roles and responsibilities of cloud provider, measurement metrics

to be evolved. The suggestion also stresses need for standardisation, transparent pricing mechanism, well documented contracts, defining mechanisms to measure SLA, providing a single point of contact, etc. As regards provisioning of computing resources and management, the suggestion identifies requirements for one time provisioning, ongoing change requests, day to day monitoring and incident reporting. The software company has also discussed requirements for ensuring portability and interoperability as well as Security and privacy of data. One of the suggestions made during the discussion on cloud option was to have ffocused group to interpret NIST's roadmap and apply it to cloud deployment for UCB segment. This group could discuss following aspects of cloud adoption.

a. Voluntary consensus based interoperability, portability and security standards:
b. Solutions for high priority security requirements:
c. Technical specifications for high-quality service-level agreements: A vendor neutral mechanism to specify and measure SLAs.
d. Clear and consistently categorized cloud services:
e. Technical security solutions de-coupled from organization policy:
f. Collaborative parallel future cloud development initiatives:
g. Defined and implemented reliability design goals:
h. Defined and implemented cloud service metrics:

5.4.3 Emerging ICT solutions for small Urban Cooperative banks

The responses received indicate that the UCB segment already has a number of solution providers providing Cloud like solutions and telecommunication companies are providing cloud carrier services. Besides UCBs many RRB and the Cooperative Credit banks in rural credit structure also availing such computing solutions. All these solution providers have their own methodologies for identification of solutions, entering into legal contracts, ensuring data security and performance measurement as well as monitoring of SLA. However, as reflected from the suggestion received from software majors who have better understanding of the potential and limitations of the cloud solutions, there is an imperative need to address the open issues and set the standards for various aspects of cloud computing like continuation of banks, SW companies as providing Cloud like solutions to the banks for sharing infrastructures.

Annexure 5.1 Responses received from the six UCBs

Particulars	Bank 1	Bank 2	Bank 3	Bank 4	Bank 5	Bank 6
CBS Implementation	2003-04	2005	2003	2006-07	Started in 1999	Initiated development of its CBS 'Genius' in 2001.
Data Centre Implementation	3 tier Data centre with DC at Pune and DRDC at Indapur since 2010.	Data Centre at Thane and DRDC at Pune since 2004	Data Centre at Pune and DRDC at Hyderabad since 2003	Data centre at Kalyan and DRDC at Pune since 2010.	Data Centre at Vashi with DRDC at Hingjevadi, Pune since 2007	3 tier Data Centre with DC at Thane and DRDC at Bangalore.
Support team	Bank employees without any external IT person.	Internal IT personnel and contract basis IT support	Managed by owned IT subsidiary	Internal IT personnel	Managed by owned IT subsidiary	Internal IT personnel
ISO certification	ISO-9001, ISO-27001	Under progress	Not certified.	Under progress	ISO 9001-2008 and ISO-27001-2005	Under progress
Shared IT infrastructure	-Since 2005 bank is sharing the DC with DNS bank -5 UCBs are using the Data Centre of the bank. -ATM network and Payment Gateway sharing in process.	ATM network sharing with 3 banks -Data centre sharing with 4 banks. -DR site sharing with 3 banks.	ATM sharing- 1 bank -Data Centre sharing proposals are under consideration.	Data Centre sharing – one bank ATM sharing – 2 banks	-ATM services -Network connectivity with backup connectivity - introducing Micro-ATM device	-ATM network sharing with 4 banks -Payment Gateway sharing with 3 banks.

Particulars	Bank 1	Bank 2	Bank 3	Bank 4	Bank 5	Bank 6
Shared software services	NIL	-IT services under ASP model, -CBS under ASP model with 4 banks. -Anti money Laundering solution with 5 banks	Proposals under consideration	ASP of software.	CBS on a SaaS basis to 22 banks. -CBS on license basis to 7 banks -Internet banking with funds transfer capability -SMS banking	CBS sharing with Co-operative banks, credit societies, and District Central Co-operative banks, State Co-operative banks, Micro Finance Institutions -Offered its software to 42 banks. On sale or ASP model.
Other services to other banks	Procurements, Delivery Channels	IT consultancy, IT support	Establish its subsidiary which provides services like end-to-end technology solutions, software development, consultancy and services, Training , System and IT audit etc.	Monitoring Technical knowledge sharing, up gradation of skill sets training,	Establish its subsidiary in 2005. -Technical consultancy for CBS implementation to 5 banks -24*7 helpdesk for CBS.	
Assurance provided to the small banks		Enter into SLA with every bank. Shares necessary part of the IT audit report with these banks. The banks also conduct their own audit of the services provided by the bank.	Enter into SLA with every bank. Shares the IT audit report with these banks.	Enter into SLA with every bank. Do not share the IT audit report with these banks.		Enter into SLA with every bank. Shares necessary part of the IT audit report with these banks.

Chapter 6
Analysis and Recommendations of the Working Group

The working group had analysed the international trends in Cloud Computing standards and developments among Urban Cooperative banking sector within India. The analysis and recommendations of the group are discussed in this chapter.

6.1 Analysis of the trends in cloud computing and its application

i) Cloud computing is an emerging option for cost effective and versatile solution for computing needs in different sectors. Different service delivery and deployment models have emerged and new types of roles of cloud service providers are emerging. The Cloud solution has many advantages since these provide business support through abstracting software and hardware components of the IT solutions to the service provider. However, there are many open issues and security issues. in cloud computing which are not fully resolved. The NIST has identified ten high level requirements as pre requisites for cloud adoption and taken up defining many standards for developing but these developments are not yet complete. The technology is therefore under development and standards are still evolving.

ii) Many cooperative banks have adopted core banking solutions using SaaS model. Given the evolving nature and complexities of the cloud computing and limitations of the banks adopting these solutions, it is likely that the rapid adoption among UCBs is more out of competitive pressures and marketing efforts rather than well informed decision as a strategic consideration and after exercising due diligence or evolving necessary risk management processes. Further given still evolving nature of legal complexities of cloud computing, the legal agreements which were prepared may not be taking into account the interests of the cloud customer banks or more so the customers of the banks availing cloud services.

iii) Although the NAFCUB has identified the service providers as ASP and fixed the fees, this was done through a competitive bidding. The technical evaluation done at the time of short listing needs to be revisited in light of various issues discussed in Cloud Computing of the report.

iv) Many large urban cooperative banks as well as software companies have been offering cloud type services on Private Cloud environment. These providers have reported that they have necessary technical capabilities and have also implemented cloud projects of various types. The bank provided cloud models have advantage of having grass root level experience and

intimate knowledge of banking, regulatory requirements and customer expectations whereas it could have limitations in terms of technological skills and exposure. On the other hand, Software specialist provided cloud models could have technological competence the solutions could be not fully suited for banking requirements. However, given open issues and risks associated with the cloud computing, appropriateness of the solutions in terms of regulatory compliance, fiduciary responsibilities, performance, scalability, data privacy and data security in multi tenancy environment needs to be examined.

v) The Software as a Solution (SaaS) model of cloud computing provides higher level of abstraction wherein the cloud user would be concerned with business aspects and hardware and software related aspects would be managed by cloud provider and business aspects by the cloud customer. Taking into account the profile of the UCB sector this cloud model could be suited for the objectives to be achieved. However, there are many process oriented and technology oriented security risks with the SaaS model and the risk mitigation for these risks needs to be implemented. Data security and ownership has been an area of concerns for many of the small UCBs as mentioned by the cloud service providers. Some banks have obtained ISO certification to convince about their quality and security standards. However, ISO certifications and process capability maturity for service providers could be necessary but not sufficient conditions.

vi) The solutions available are not having any benchmark standards with which they can be evaluated for quality and security. Although the cloud solution providers had mentioned their own standards for development, cloud deployment and service delivery, they had not indicated whether their solutions had been accredited for functionality, quality and security. Also they had also not mentioned about any audit certifications or IT audits through independent auditors. There was no clarity regarding compliance to regulatory requirements and these solutions were not subject to any supervisory review. Thus, while players like Cloud providers, cloud customers, cloud carriers had already evolved, the role of Cloud auditor as mentioned in the reference architecture has not yet evolved. The software industry participants have expressed concern over this and have expressed need for standards and processes for cloud technology management.

vii) Despite of limitations in respect of exposure to complexities of cloud computing at the decision making levels, legitimate and valid concerns for data confidentiality and privacy in multi-tenancy environment were expressed

by the decision maker small Urban Co-operative banks while discussing the proposals offered by the service providers. Given the commercial interest of the cloud providers and increasing digital divide between those to whom the Cloud solutions are intended and those who are now equipped to design and implement these solutions, there is a risk of opting for cloud computing option on partial or incomplete understanding and also based on selective information.

6.2 Recommendations

The working group reviewed its terms of references in the context of the emerging trends and experiences and views of the CSP. Following recommendations are made in this context:

- As cloud computing is an emerging technology for which standards and technology management processes are still evolving. It has many complexities and uncertainties which need to be understood. In view of the sensitive nature of banking services as well as limitations of the target banks for managing this technology, the Working Group recommends caution while adopting cloud computing solutions for the target Urban Cooperative banks till such time that issues are resolved satisfactory.

- In respect of banks where such innovative Cloud like solutions are already deployed on a Private Cloud, the Working Group recommends that the issues identified in this report may be examined on the lines indicated in the report to ensure adequacy of risk mitigation measures and to address concern regarding data security and data privacy in the multi-tenancy environment.

- Despite its evolutionary stage, cloud computing offers new means in many support and surrounding services in banking which could be identified and non financial applications could be ideal candidates for cloud computing solutions to be tried for gaining more experience. This could be a developmental activity which can be taken up separately and the experience in this regard could be shared to understand the intricacies of the cloud solutions.

- As revealed from the experience outside India as well as the suggestions received from the major industry players, the Working Group perceives a need for further research and development particularly in the area of cloud governance, cloud management and security technology for cloud computing. Initiative in this regard probably needs to be from the banking and software industry whereas the regulatory authorities could make use of such research input at a later date.

(A. K. Hirve) **(G. Shivakumar)** **(H. Krishnamurthy)**

(A. Udgata) **(S. Ganesh Kumar)** **(Deepak Hoshing)**

(Ujjwal Mathur) **(Satya Mishra)** **(Jitendra Chivate)**

The Working Group would like to thank different Urban Cooperative Banks as well as the IT solution providers for their input and valuable suggestions. The group acknowledges the help received from the officers of Department of Information Technology RBI namely Shri Hemant Kumar, General Manager Shri T.K. Rajan, General Manager, Shri Sachin Shende, Deputy General Manager, and Smt Shubhangi Latey, Assistant General Manager for their analytical support and their efforts for timely completion of this report. The group would also like to thank Smt. Vibhuti Mohite for her secretarial and other support for the study.

References

1. Special publication 800-146 NIST National Institute of Standards and Technology U.S. Department of Commerce http://www.nist.gov/.
2. Special publication 500-196 NIST National Institute of Standards and Technology U.S. Department of Commerce http://www.nist.gov/
3. Special publication 500-193 NIST National Institute of Standards and Technology U.S. Department of Commerce http://www.nist.gov/index.html.
4. Special publication 800-145 NIST National Institute of Standards and Technology U.S. Department of Commerce http://csrc.nist.gov/.
5. Guiding Principles for Cloud Computing adoption and Use http://www.isaca.org
6. Control Objectives for Cloud computing http://www.isaca.org
7. ValIT Framework 2.0 http://www.isaca.org
8. Security Guidance for critical areas of focus in cloud computing version 3.0

   https://cloudsecurityalliance.org
9. What is cloud computing and its background http://en.wikipedia.org/wiki/Cloud_computing
10. What is cloud computing and its background http://www.guardian.co.uk/cloud-computing/what-is-cloud-computing