# Security and Policy - A Major Concern and Hurdle In The Widespread Implementation Of Cloud Network In Public Sectors

**[1]Narendra Kumar, [2]Dr. Saket Bihari Singh (Ph. D.)**

[1]Research Scholar, [2]University Prof. of Mathematics
Magadh University, Bodh Gaya

***ABSTRACT*: Today Cloud environment has becomes essential need and choice of every sort of organizations due to its efficacy, lower cost and ease of its implementation. Migration to the cloud computing environment has also become simple and effortless. Its nature of simplicity, cost-effectiveness and hassle – free service also attracts some major security issues on and after its implementation, particularly, in Public Sector Organizations.**

**Major public sector organizations and Govt. agencies reported that they are either concerned or very concerned about the potential information security risks associated with cloud computing. Risks include various sorts of dependencies on the security practices and sharing of computing resources in several modes. If agencies publicly disclose which cloud providers they are using, hackers tend to immediately seek to penetrate the provider's security measures. And if multiple agencies are using the same provider, then a breach of one will be a breach of all. Thus, it's imperative that agencies stay mum about not only which cloud security solutions they're leveraging, but what data they are looking to protect. There are various ways through which for hackers to break the code and bypass the cloud security barrier. The public sector organizations and Govt. agencies have a high degree of risk factor in migrating their IT based services to the cloud provider.**

**Many developed countries such as United States of America, Japan, United Kingdom, France and major economically and technically developed countries has migrated their public sector department to the cloud environment taken several steps on security policies and still working on security measures to provide full proof security to the public sector cloud computing environment. In Asian subcontinent, including India, the cloud implementation in public sectors has just initiated for the last five years and countries in this subcontinent has wide range of public sectors and govt. agencies which are potential users of Cloud Computing. At the same time the security and privacy issues are the major concerns for these organizations. The presented paper mainly deals with the security issues related to the public sectors and highly sensitive security agencies in Migration and Implementation of Cloud Based Infrastructure. The presented paper also suggests a considerably secure way to gradually migrate and implement Cloud Based Services in public sectors and sensitive Govt. departments.**

**Index Terms: Cloud Security, Public Sector Cloud, Virtualization, Encryption, Govt. Agencies**

## 1. Introduction

The definition of Cloud Computing varies slightly according to the position and perspective of an institution on Cloud Environment. Cloud Computing can be defined as "the large-scale distributed computing service environment in which as much of the massive IT resources including computing power, storage, platform, and services as required are provided for different sorts of organizations through the Internet." Cloud computing is so named because the services and information being accessed is found in the 'cloud', i.e. Internet environment, and does not require a user to be in a specific place to gain access to it. Business organizations today greatly reduced their cost of managing the data and computing infrastructure, since they are not required to own their own servers and can use capacity leased from third parties. Almost every day private companies, public sectors bodies and small business organizations are migrating their IT based services to the cloud infrastructure throughout the world.

Cloud computing is a disruptive innovation that expands its frontier with each evolution of technology. Although the idea of hosted applications emerged in the 90s, it was not until the rise of web-based Software as a Service (SaaS) that the model became a viable component of enterprise architecture. A decade later, enabled by advances in technology, SaaS vendors have expanded their portfolios, and new entrants have pushed the cloud deeper into IT organizations with the addition of new service classes, broadly:

- **Software as a Service**. Delivers software over the internet using an "on demand" model that frees customers from having to manage the supporting environment. e.g., Cloud9 Analytics, Financial-Force, Oracle, SAP and salesforce.com.
- **Infrastructure as a Service**. Delivers computer infrastructure—typically a virtualization environment as a service. e.g., Google ComputeEngine, Rackspace

OpenCloud, IBM SmartCloud Enterprise, Amazon AWS, etc.

- **Platform as a Service**. Delivers both a computing infrastructure, and solution building blocks (development environment, data access library, testing tool), as service. e.g., Engine Yard, AppFog, Caspio, Google AppEngine, etc.

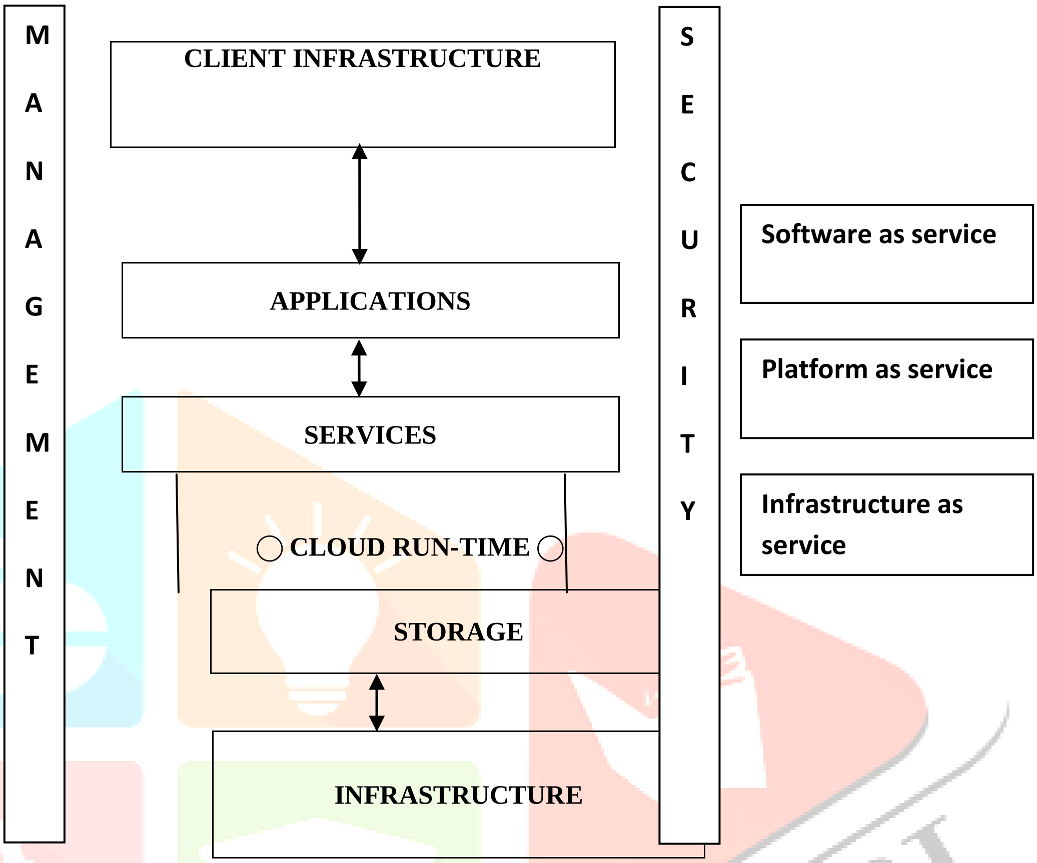

**Fig. 1 BASIC CLOUD ARCHITECTURE**

## 2. Necessity of Cloud Implementation in Public Sectors and Govt. Agencies

Whereas small, mid-sized and large organizations may leverage public cloud infrastructures offered by IBM, TCS, Microsoft, Amazon and Google, now here is the opportunity to create, leverage and benefit from private and hybrid clouds as great as within the world's largest organizations: the public sector and Govt. agencies. India has nearly 3.2 millions of Central Govt. employee operating throughout the country, with about more than 6 millions of employee working with state public sectors units. In the United States of America, about 2.79 million employees are working with federal states and local bodies. Russia has about more than 2 millions of government and public sectors employee, China with 39 millions of civil servant and public employees. With approximately 250,000 employees operating in more than 150 countries, the federal public sector of Canada is the largest and most complex employer. With such size and scope of services, the agencies that comprise the public sector and Govt. agencies are ideal entities for cloud computing architecture.

## 3. Major Implications in Cloud Migration and its Implementation

**3.1 Access and Authentication Policies:** This is a major concern in the implementation of cloud in the govt. agencies and public sector departments. The cloud providers/architecture may not be in conformity with the Govt. policies, regulations and legislation about data access and security. On implementation of cloud deployment, the data governance becomes a major issue because data are stored outside institutional and territorial boundaries. They have a 'fear factor' concern with security and accountability issues. Data security is still an ill-solved issues in the cloud computing world and when we talk about largest potential users – public sectors and the Govt. agencies, the issues becomes more critical. The sensitive data and information must be available for the intended users only. The Cloud Service Provider must be made accountable for the unauthorized access of personal and sensitive business data.

**3.2 Interoperability:** The Govt. agencies and public sector departments may coordinate with multiple organizations and the cloud infrastructure may have products of different vendors and manufacturers across the globe. Definitely, the potential users seek seamless interoperability of the cloud based services.

**3.3 Security Policies:** Hacking and stealing organizational sensitive data could create high degree of complications in term of National Security and the trust factors to the general public. As the Cloud Providers are developing and using more sophisticated ways to provide security to the sensitive data, the hackers are also using new techniques to steal sensitive information. Due to privacy and security concerns, 87 percent of Govt. Agencies in US are very afraid to use Cloud for their sensitive business data. (As per Survey)

**3.4 Control over System and Resources:** It's a big question and concern that who will have control over the data and resources and how? The public sectors and Govt. agencies data and other resources are very sensitive and some of them may raise threats to the National security. The Cloud Service Provider's IT and Computing resources are polled to serve multiple consumers. Different physical and virtual resources are dynamically assigned and re-assigned as per the demand.

**3.5 Compliance:** For the cloud venders, this is perhaps most important to conforms to all the Govt. rules and policies for services rendered through the cloud environment. The cloud venders need to analyze and prepare to be ready to provide the services under the policies defined by the government.

**3.6 Risk Assessment:** This is another major hurdle in the migration of public sectors to the cloud infrastructure. The problems

and risk must be anticipated to face sudden breakdown of cloud venders and risks that might come into existence during migration or after the migration.

**3.7 Migration Strategies:** This is another critical issue in cloud implementation for the public sectors and Govt. agencies. The migration of resources to the cloud environment has several operational, cultural (Office Procedures), reliance and compromising factors.

## 4. Sociological and Regional Issues:

**4. Sociological and Regional Issues:** Besides, there are a number of imperative concerns and fears of unknown implications when Public sectors and Govt. agencies consider a Cloud migration and implementation. So, Public sectors and sensitive agencies have massive trust deficit issues while moving to a Cloud environment.

**4.1 Senior Management Engagement:** It is important that leadership of organizations understand the value of these technologies, evolve specific initiatives that deliver superior services, profitability, brand value, etc. They need to lead from the front in pushing the adoption of these technologies in their organizations within defined timelines.

**4.2 Lack of Trained Staff:** IT is getting intertwined with functions. The best use of IT cannot be delivered by a disconnected or siloed MIS Department. Leadership has to enable and build crack cross-functional teams to design their digital and cloud roadmap and deliver the same.

**4.3 Legacy of Hard Copies:** Hard copies are still preferred mode of data by the top managers and policy makers of an organization. They hardly believe on the Cloud Infrastructure and services and very concern over the security of data.

**4.4 Procurement Methods:** The approach of buying the lowest cost option through a tendering process, does not necessarily result in the best procurement of IT products & services.

**4.5 Constraining Implementation Guidelines:** Complex tender conditions, with limited flexibility downstream in implementations, resulting in poor success rate of implementations. New initiatives with new technologies do run into challenges at times. The ability to adjust downstream is a must for success of such initiatives.

## 5. Latest Research in Cloud Security:

Several giant computing companies across the world are involved in the research and development of full proof security measures. Some of the major researches carried out by different vendors are:

**5.1 INTEL and VMWARE:** Intel has developed Intel Trusted Execution Technology (Intel TXT), a platform for trusted cloud that integrates VMWare's vSphere, a well known platform for building cloud infrastructure. vSphere provide high integrity platform to run Business-Critical-Applications.

**5.2 MICROSOFT Research:** Currently Microsoft is working on Homomorphic Cryptography which includes Fully-Homomorphic Encryption (FHE), Somewhat Homomorphic Encryption (SHE), Searchable Encryption, Structured Encryption, Functional Encryption and Garbled Circuits.

**5.3 IBM:** IBM introduced pervasive encryption that provides full encryption of application, database and cloud services with the new pervasive encryption technologies.

**5.4 Infosys and Queen's University:** Infosys and the Queen's University Belfast's has signed a major strategic partnership to combat security threats in cloud computing. Infosys and Queen's University (Centre for Secure Information Security) working jointly on a wide range of Cloud Security Services and expecting potential outcome.

Besides, various similar computing giants such as Rackspace, Wipro, Google and Adobe and are engaged in the research and development for secure cloud environment.

## 6. Migration Strategies:

A well defined and anticipated strategy could lead to a better migration and deployment outcome. The 'SECURITY' and "POLICY" are two major concern that public sectors and Govt. agencies has to be cope with. Several migration techniques evolved in the last ten years and still scientists are working over the migration strategies. There may be two options in this regard:

a) Migration and Deployment with Service Provider's Private Cloud or Hybrid Cloud.
b) Migration and Deployment on its own Private Cloud, available with full control.

In both of the cases, the security issues come over the floor and here several complexities started to popup. The Migration and Deployment strategies are beyond the scope of this paper.

## 7. References:

**[1] Susmit Bagchi, "Emerging Research in Cloud Distributed Computing Systems", published on March – 2015, pp. 201-208.**
**[2] Joe Weinman, Cloudonomics – The Business Value of Cloud Computing, 1st Edition, published on Aug – 2012, pp, 194 – 201.**
**[3] David A. Powner, "Information technology reform: Progress Made but future cloud computing Efforts Should be Better Planned," United States Government Accountability Office, GAO-12-756, pp, 1-38, Jul. (2012) (Accessed on: 22nd – Oct – 2017)**

**[4] David C. Wyld, "The cloudy future of government it: cloud computing and the public sector around the world," Internal Journal of Web & Semantic Technology, pp, 1-20 (2010).**

**[5] https://www.microsoft.com/en-us/ research/ project/cloud-security-cryptography/**

**[6] Scott Campbell – Federal CIO:" Government needs to rethink technology for 21st Century" – ChannelWeb – 30th April – 2009 (Online mode). Accessed on : 28th – Sep. – 2017**

**WebLink :http://www.crn.com/news/the-channel-wire/217201051/federal-cio government-needs-to-brethink-technology-for-21st-century.htm**

**[7] Ronald L Krutz, Russell Dean Vines: Cloud Security: A Comprehensive Guide to Secure Cloud Computing - Wiley (2010)**

**[8] Tim Mather, Subra Kumaraswamy, Shahed Latif : Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice), O'Reilly Media; 1 edition (October 5, 2009)**
**[9] John Rhoton, Cloud Computing Explained: Implementation Handbook for Enterprises, 1st edition, Recursive Press (November 2, 2009).**