Proceedings of GLOGIFT 17
December 11-13, 2017
Delhi School of Management, Delhi Technological University, Delhi
pp. 686-690

Flexible Management through Secure Digital India Initiative of the Government

Archana B Saxena[1] and Sanjive Saxena[2]

Introduction

Digital India, an initiative launched by the government of India with the intention to transform India and link the country with the digital empowerment of society and knowledge-based economy [www.digitalindia.gov.in]. This program, which is more than lakh crore has three major targets *viz.* Digital Infrastructure for every citizen which will provide several utility services of the government, promotional of Digital literacy to next level and provision seamless integration across several departments across many jurisdictions with information and communication technology forming the backbone [Lakshmi, Vijayalakshmi, and Ugrappa. (2016)]. The e-education, e-health, e-sign are some of the schemes launched under this initiative whereas UMANG (Governance), UDAAN (Unemployment in J&K), SWAYAM(students), SWATCH BHARAT (Cleanliness), SUGAMAYA PUSTKALYA (online Library), SARANSH (CBSE affiliated schools) are the services. [www.digitalindia.gov.in].

In order to ensure that this initiative is successfully implemented, the fundamental requirements must be put in place first. These include a strong and robust Information Technology infrastructure, provision for storing large amount of data which would be generated from the various operations and services of this initiative and above all it requires a sustainable training, education and awareness program to ensure that rural and urban citizens are able to adopt the benefits of being Digitally empowered efficiently and effectively. Cloud computing, a relatively new technology, provides requisite infrastructure along with the added benefits of cost savings to make Digital India, a dream come true. For, Cloud computing, operates on the backbone of Internet and thereby links several Data Centers of the government departments and integrates them by network resource centers. In essence, Cloud computing has three major components:1. Infrastructure as a service, 2. Platform as a Service and 3. Software as a Service. These are commonly abbreviated as IAAS, PAAS, and SAAS. The word *service* denotes the concept of pay per use structure. In other words, the customer pays to the cloud service provider the amountof money for the time which he uses. He is not required to incur extra cost on hardware-software or on the maintenance or any other cost such as licensing and procurement. According to E-tech India summit, (2015) the incorporation of appropriate encryption technology, Cloud Computing will be the next step in integrating the country for Digitalization [www.indiatvnews.com].

1. Jagan Institute of Management Studies, Near Rithala Metro Station, Rohini, Sector-5
New Delhi-110085
Phone: (M) 0- 9818554220, Email: Archanabsaxena@gmail.com
2. Jagan Institute of Management Studies, Near Rithala Metro Station, Rohini, Sector-5
New Delhi-110085
Phone(M)0-9868515570
Email: sanjive.Saxena@gmail.com

Necessity and contribution of Cloud Computing in the success of Digital India scheme are well registered but security lapse and data leakage form cloud is raising few questions that must be answered before commonalities will adopt this scheme without any apprehension. Worth mentioning a recent data security lapse, where an IIT graduated student is arrested for unauthorized access of "Aadhar card database", one of the important components of "Digital India" scheme [Johnson (2017)]. With such incidents it quite obvious to have reluctances among service consumers towards "Digital India" schemes and services. Various queries related to availability, integrity, and security of data goes around in customer's cognizance. Who is responsible for the security of data or information saved under schemes or services launched by Digital India notion? What efforts is the government taking to ensure the security of data? Is there anything we can do to save our data and much more?

All this boils down to the basic concept of "***flexible Management of stakeholders***" in the digital India campaign. This paper is thus an attempt to address some of the apprehensions through our current paper by accumulating issues that can affect IAAS security and impact security of data saved in "Digital India" scheme, measures that can be used to control security lapse. Digital India scheme has various stakeholders like Government, Service Provider, Service Consumer. Authors have a perception that security cannot be ensured through one but it should be a contributed effort by all stakeholders. Keeping this in mind responsibilities are defined for stakeholders they should be responsible to implement defined security measure and hence contribute in taking "Digital India" a step ahead.

Keywords: Cloud Computing, Cloud Security, Cloud Stakeholders, Digital India Security, Flexible Management

Research Gap and Research Problem: From above discussion, it is evident that IAAS of cloud computing is considered as the base and must ingredient for smooth functioning of Digital India and it is thus required to managed flexibly. Any challenges faced by this technology will directly impact working of this government scheme. A lot of discussion has been carried out by researcher across the globe related to Cloud Computing and Digital India management, such as:

Lakshmi, Vijayalakshmi, and Ugrappa (2016) has covered "Digital India" in details like information about program, services, schemes, budget, and beneficiaries of the program. A good coverage of mission, methodologies, impach and relation with E-governance are also highlighted in the paper.

Ganeshkumar and Ramesh (2017) have proved through data collection and analysis that cloud services can be useful in supporting "Digital India" schemes. They have used various techniques like k-means, clustering and regression algorithms to analyze twitter data and give recommendations.

Siwach, Jyoti and Amit Kumar (2015) have referred Digital India as dream project for government of India and explained how digital innovation can have positive impact on lives of urban and rural population. They have also emphasis on the challenges faced by this dream project.

Modi, Chirag (2013) have explained challenges faced by different layers of cloud and impacting its adoption among commonalities. They have also enlist the measures that can be used to enhance privacy and security of cloud.

Kaufman, Lori M (2009) have discussed need and measure to ensure data security in the cloud. The impact of security on trust is also dicuused in the detail.

Ramgovind, Sumant, Mariki M. Eloff, and Elme Smith [2010] have kept an aim to provide overall security to cloud computing and to achieve this aim they have discussed joint responsibilities in ensuring security in the cloud.

In this paper we develop following research problem to address flexible management in the digital India campaign and try to address the various issues related to it:

a. The degree and extent to which Digital India is secure with respect to its various operations pertaining to stakeholders.

b. The degree and extent to which Government, Service Provider and Service Consumer realize their responsibilities in securing "digital India" campaign and implement flexible management controls.

Although the sound literature has found related to "Cloud Security" and "Digital India", still following gaps have been identified in the literature:

a. There is no discussion about Security issues of cloud computing that can directly impact "Digital India" notion and hence they must be managed

b. What measures can be used to ensure the security of data or information saved on cloud and finally ensuring secure transactions in digital India? In other words flexible management by using these measures

c. Who is responsible to ensure the security of data or information saved in the cloud under "Digital India" scheme? Again, a management issue which can be implemented flexibly.

Objectives of the study: To bridge the gaps identified in literature author have kept a few fold objectives for this paper:

a. Security threats of IAAS that can impact "Digital India" Schemes and Services.

b. Measures that can be used to overcome above mentioned challenges/threats.

c. Generating a task list to implement security measures.

d. Segregating task list between stakeholders and Defining of responsibilities of each one to implement secure "Digital India" scheme.By achieving above mentioned objective authors are trying to achieve the prime objective: making "Digital India" a secure practice and contribute in nation development through digitization empowerment.

Research Methodology

In order to achieve mentioned objectives, initially, authors have defined the scope of the study, by selecting cloud service that can be a support for "Digital India" operations. So, the scope of our study is related to IAAS service of the cloud.

Once domain pertaining to the study is defined then author have followed a structured approach to the development of this paper. To define the challenges of IAAS that will impact "Digital India", data is collected through primary and secondary means. For secondary data collection: the internet, online newspapers, journal, research paper are used. Primary data is collected through structured questionnaire. Few samples are collected online from IAAS users. Collected samples are filtered, verified and validated before analysis in excel. After finalizing the issues that can impact IAAS security. The next step is to finalize, "Security Measures" to resolve above-mentioned issues. This chore is accomplished through literature survey, discussion with SME (Subject Matter Experts) and authors own knowledge about the topic. Once security measures are identified then task list is concluded to implement these measures and finally responsibilities are segregated between stakeholders to implement defined task in order to ensure security.

Findings of the Study

Findings will present a list of IAAS security challenges that can impact "Digital India" schemes and services. Another list that is pertaining to study is the list of measures that can be used to control or avoid security lapses like Certifications, standards, and technical update that ensures security coverage at IAAS. Once the security measures are identified then task list is created to implement these security measures. Ex: ISO/IEC 27002 for proper protection of data or information, strict authentication, and authorization mechanisms for data access and modification, strict rules and laws pertaining to cyber security, and much more. These tasks/ responsibilities are further segregated among stake holders [Government, Service Provider, and consumers] and make them accountable for these chores and request them to contribute in security project.

Implications of the Study

World Bank predicts that with success of "Digital India" country will be a third largest economy in next 10 years [Johnson, (2017)]. As an IT professional and researcher, it is our moral responsibility to contribute to literature to convert World Bank's prediction into realism. Our study contributes to the literature, various responsibilities that each stakeholder should carry out to ensure the security of data and information saved on cloud and hence protected "Digital India" scheme. An implementation with the right approach and existing literature our study can contribute in following ways:

a. "Digital Literacy": Secure and comfortable services will lure every citizen and masses will accept it.

b. "Digital Empowerment": Secure IT infrastructure will boost up digitization of all government departments and jurisdiction.

c. Secured IAAS service can distribute IT infrastructure among masses without huge investment and security apprehension.

References

- Johnson TA (2017), "IIT Kharagpur graduate hacked Aadhar data through Digital India app: Police", retrieved from http://indianexpress.com/article/india/iit-grad-his-firm- booked-for-hacking-aadhaar-data-4772220/
- Siwach, Jyoti, and Amit Kumar. (2015) "Vision of digital India: dreams comes true." *IOSR Journal of Economics & Finance* 6.4(2015): 66-71.
- Ganeshkumar, M., and V. Ramesh. (2017) "A Study on Digital India Programme Using Azure Cloud and Twitter Data." *International Journal of Computational Intelligence Research* 13.5(2017): 781-790.
- India TV News desk (2015) "adoption of cloud computing is the next step of Digital India", retrieved from http://www.indiatvnews.com/business/india/adoption-of-cloud- computing-is-next-step-of-digital-india-19853.html
- Lakshmi, A., S. M. Vijayalakshmi, and E. Ugrappa. (2016), "Evaluation of Digital India Programme." KHOJ: Journal of Indian Management Research and Practices: 277-281.
- Ministry of Electronics & Information Technology Government of India website about "Digital India" program retrieved from http://digitalindia.gov.in/content/introduction.
- Modi, Chirag, et al. (2013) "A survey on security issues and solutions at different layers of Cloud computing." *The Journal of Supercomputing* 63.2(2013): 561-592.
- Robert LeBlanc (2015), "Intelligent cloud will define Digital India's Success", retrieved from: http: // www.livemint.com/ Opinion/ JhJdtYSpPp1TSxVmP90fHO/ Intelligent- cloud-will-define-Digital-Indias-success.html

- Jain, R., S. Madan, and B. Garg. (2016) "Privacy sustainability scheme in a cloud environment." CSI transactions on ICT 4.2-4 (2016): 123-128.
- Kaufman, Lori M. (2009) "Data security in the world of cloud computing." IEEE Security & Privacy 7.4.
- Prasad, Kiran. (2012) "E-governance policy for modernizing government through digital democracy in India." *Journal of Information Policy* 2(2012): 183-203.
- Ramgovind, Sumant, Mariki M. Eloff, and Elme Smith. (2010) "The management of security in cloud computing." *Information Security for South Africa (ISSA*),2010. IEEE.
- Zapolskas, Vytautas. (2012) Securing Cloud Storage Service. *MS thesis. Institute for Telematics.*Wei, Lifei, et al. (2014) "Security and privacy for storage and computation in cloud computing." *Information Sciences* 258(2014): 371-386.