

An Analysis of Security Threats in Cloud-Enabled E-Governance Models

Sapanjeet Kaur

Assistant Professor, Mata Sahib Kaur Girls College, Talwandi Sabo

Abstract: The cloud computing model provides the software, platform and infrastructure through the internet as web services. The cloud user obtains hardware and software from cloud service provider and treat all the resources as its physical assets. The services of government provided to the citizens, business and government easily and in less time through the E-Governance. Cloud computing also provides a platform for efficient development of E-Governance. It helps to establish an environment which is user friendly and all the resources are provided on the basis of demand in distributed environment. The information security is an essential tool to reduce the risk at all levels of data sharing. Cloud also utilizes resources by representing the distributed computing of E-Governance services. The cloud based E-Governance collaborating the applications of government boundaries through the network and utilization of resources among all the service users. The cloud based E-governance may be having some challenges but these challenges would not criticize the architecture of cloud. It would seem to be a secure and reliable environment for the citizens. It encourages the user to share and access the resources on cloud based framework of E-governance.

I. INTRODUCTION

The advancement in internet facilities become life more convenient and provide the way to use the resources efficiently. This facility was not provided few years ago, in traditional system the sharing of data and resources was difficult as well as time consuming process. Cloud computing is one of the emerging technology in recent years. The term "Cloud Computing" states to a range of Internet-based computing services. The cloud computing is nothing but a new technique to deliver the information to the use by utilizing the existing technology and resources. It is very cost effective and flexible alternative to access the hardware and the software in user's system. The cloud also offers the infrastructure as well as concerning software, storage, networks and other fundamental services. The Google App Engine, Microsoft Windows Azure and Oracle Public Cloud are helpful to provide the required platform to the users. The supporting software are provided by the Google Apps, Microsoft Office 365, Salesforce.com. amazon is pioneer in cloud computing service providers. The Amazon Web Services(AWS) is a platform which consist of huge amount of web services, and obtained by the users on demand basis. The client of amazon demand for the higher level of security for their data because of its financial

transactions(Amazon,2012). Google is also in the race of cloud providers. Google App Engine provides application development and hosting environment. Multiple servers are hosting the in Google data centers to fulfil the requirement of users. All these organizations attempt to increase the probability of data security in different clouds. As with security there is no real evidence that placing sensitive information into cloud environment and the risk of unauthorized access of the information is reduce. In some cases, find the protocols of various national and international data protection.

II. CLOUD BASED FRAMEWORK OF E-GOVERNANCE

The services of government provided to the citizens, business and government easily and in less time through the E-Governance. But all this is not enough to satisfied the requirement of the government users. So cloud computing also provides a platform for efficient development of E-Governance. It helps to establish a requirement based environment which is user friendly and software and hardware both are providing as a services to the users. The E-Governance adoption is heavily investing and more sophisticated process to deliver the services. It also faces some technical and non-technical problems while performing the services. The technical issues are poor broadband internet access, limited access, late adoption of new technology and lack of new knowledge. And the another critical problem is security related issues. In the developing countries, implementation of E-Government is challenging aspect. The protection of electronic data is also a matter of concern for the countries which adopt the E-Governance. The information security is an essential tool to reduce the security risk at all levels. Cloud also utilizes resources by representing the distributed computing of E-Governance services. But in such type of distributed environment security is the main concern.

III. REVIEW LITERATURE

There is enormous research that describe the cloud based framework and E-governance model. Some of them also designate the framework to provide a secure and reliable environment. The previous studies also explain the type of security at different levels of transaction. Cloud computing is a new technology and a model which deliver the information by using the existing facilities (Carlin and Curran, 2011). Cloud computing is the collection of resources that are helpful to

increase efficiency, reliability, security and quality by providing services with efficient use of sharing equipment (Vouk,2004). As mentioned in previous chapter, security is the main concern in cloud computing. The cloud adopting organization realize the benefits of it, the services are provided on less cost through existing resources. So it is not necessary for the users to spend money on resources and other helping software while it is available on cloud based infrastructure. This sharing environment is similar to the time sharing technology of 1960s. So many of the security issues are similar to that era, when the internet is expanded to share the data from client to server. But in this thesis describe the security problem faced by the cloud based e-governance environment. The cloud provides a virtual environment on the demand of user. In this virtual machine the software program on host machine help to provide and control the sharing of resources among all users (Krutz and Vine,2010). Only the machines isolate with cloud access the services from the host, but some time those who are not isolate with particular cloud would demand for the resources and break the security and privacy to perform such task. The another type of attack is hacking, the password and user name would hack to perform unauthorized access. This process is also known as keystroke timing attack. In this the attacker measure the time between the keystroke. Each key is send on different package to server, so it is easy for the hacker to guess the length of each key and access the secret information or data (Song et al.,2002). To solve this problem access control is implement. The unauthorized access can be detecting through this mechanism. It provides the best result to reduce the intentional and unintentional modification in data. The access control also helps to prevent the data from unnecessary change and loss of data while transferring from one device to another (GAO, 2011).

The data is protected by identity management in governance process, which creates a balance between the risks arises in access the information in advanced technology. The Smart citizen card also a good concept to identify either the user is reliable or not. The authentication and authorization of citizen identify electronically to use the services of E-governance. The another technology is department specific ID, which assigned to different department of the government such as income tax (IT), health and social welfare department (HS) etc. Each Department Specific PIN (dsPIN) is different alphanumeric code to access the services, and then apply a cryptographic one-way function to secure the data (Pandey et al.).

The information is travel on different network equipment while transferring to server data center to client data center in cloud based E-governance architecture. So the security at each level is must to protect the data from unauthorized access. The involvement of advanced technology reduces the total cost of providing the services to the citizens. The virtualization in

cloud computing architecture enhanced the accessibility of services. The Information and Communication Technology (ICT) is playing a vital role in delivering of e-services at grass root level to proper utilization of resources and use the free and open access software for development of E-governance projects. It reduces the financial burden abide by the state and central government to satisfied the citizen and best delivery of services at root level (Puneet et al.,2013).

IV. SECURITY CONCERN IN SHARABLE ENVIRONMENT

E-Governance faces some technical, networking and non-technical problems while providing services to the users. The biggest issue is the advancement in technology, the hardware and application supporting software are changed at rapid rate. So the replacement of these resources is too much expensive as well as time consuming process. The implement of new hardware and software instead of existing one is a major technical issue. The cloud provides the environment where the E-Governance applications run on new technology, but no need to upgrade the existing system. The resources are shared on cloud on demand basis. E-governance departments may not want to purchase the expensive technology to run the applications. All the services can be run on a sharable setup, where the users and provider both take advantages from the resources of others and after completion of service they can pay only according to the time of use resources. The cloud provides the services on large scale and the E-Governance also satisfied the huge set of service users.

The cloud provides every facility as a services to the users. In the cloud based E-government the hardware, software and network all the resources provide by the cloud to run the E-Governance application. All the services of E-governance need a huge amount of data and need a large storage space. For this cloud provides a common infrastructure to utilize the resources and make the application easy to run. It supplies CPU, storage structure, bandwidth and other useful resources as a service. Cloud also provides standard system software that are helpful to execute E-Governance applications. The E-Government departments request for Employee management system, water boards, billing, E-Polices, E-Courts, and attendance resolutions system as a service and cloud provides it on demand. Some platforms also supply by the cloud as a services to the E-Governance applications like databases, operating system provisions, middleware services, and workflow services. Cloud provide a virtual environment to every user to developing the E-Governance applications. With the help of cloud, the services of E-Governance become more beneficial, easily accessed, less implementation expensive, more reliable, and less time consuming.

However, the cloud is attracting the E-Governance to provide services to the citizens by a virtual environment and the

infrastructure also established on demand of service user. E-Governance services contain a huge amount of data related to particular application. Hence the most useful and personal data also on the cloud database. For all this security is the major concern to set a cloud based environment for all services of government. The storage structure of data and access control is the key concern. The hacker who has been interested to access information for personal benefits is also a big challenge faced by the cloud service provider. The data also classified according to the requirement of user. Data is separated from user to another and also set the state of data either is in transit or at rest. The different service level agreement (SLA) also specify the contract between service provider and service users. It describes the level of service which provide to the users. Many of the cloud provider also promote the secure, reliable and easy to access virtual infrastructure to the users.

The subsequent growth in cloud computing has brought a great change in storing information and computation task. The government also take initiatives to change the technique to provide the services to the citizens. Cloud based E-Governance contains critical application programs and have sensitive data for performing operations through internet.

The biggest issue is to share and available the data on public cloud because most of the government services are provided publically. The citizens get advantages from these online services to make their transaction easier, reliable and less expensive. The government use the public cloud to satisfied the users and fulfil their requirements in the form of data, platform, infrastructure, supporting software, hardware and other needed resources. The service provided by the Cloud based E-governance is the combination of computing concepts and technologies such as Internet, Web 2.0, Service Orientated Architecture that are supportive to fulfil the need of user. The data and the software which are beneficial for the whole processing are stored on the servers. In the same respect as the clouds are good approach for providing services, there are some problems are also occurring while adoption of the system.

Challenges to deliver the services in cloud computing structure Cloud provides the infrastructure to share the resources and services to clients and establish a connection between server side and client side for communication. But security is the major problem at both the ends of the service provider as well as service user. The security of data and resources is necessary at all level of transaction such as data storage, network, application software and access control of data. All the services of clouds are dependent upon each other for make the environment more reliable and secure. PaaS helps SaaS by providing an environment to perform any transaction without any obstacle and help to increase the level of security in provided services. The security increases the availability of

confidence in user to share the resources and data on internet for efficient use and enhance the strategy of resource sharing. The security is essential in cloud environment where different users share the resources. But there are some security attacks are occurred while data and services are provided on cloud based framework of E-governance:

Internal attacks: - The cloud service providers are not trustworthy in some situations. Some internal workers also leak the secret information of user for personal benefits. Not all the members are in working environment are faithful. The personal information can be misuse by the unauthorized parties. E-governance services provided on internet have huge amount of personal data of citizens while they use service or fetch the data from service provider and submit required personal information which related to the transaction. The information of individual can be requested and passed to the other parties on sharable environment.

Integrity of data: - The service provider should be sure about the integrity of data storage, transfer and retrieval. It means only authorized parties can change the data and perform any transaction on it. but it is very difficult to maintain the consistency of data in virtual environment where same data is accessible by multiple users.

Control of Encryption keys: - The encryption and decryption keys are mostly control by the customers. They can also use it either to violet the privacy rights of information or damage the data for personal benefits and access the secret data by frauds.

Incompatible venders: - The storage services can be provided by one vender to another on demand of users in some transactions. But sometimes these venders are incompatible to each other and it is very difficult to move the data from one vender to another.

Network security: - In sharable environment the security of network setup is also a major issue. The users can deny to access the services of particular network due the harm of security of information and resources. The service users are not sure their information is secure or protected on particular environment.

Lack of confidence: -The users are not confident to share their private data on network. They are not sure about the privacy and security of data and resources. They have no idea how the service provider enables to set a secure and comfortable environment to share resources. In government transaction resources are accessed publically and secure them from harmful or unauthorized parties is main issue.

Multi-tenancy: - In cloud environment multiple clients are using the same resources simultaneously. So it is very difficult

to satisfied all the clients at same time. So the process scheduling is required for performing all the transactions.

Data Management: - in distribution environment the management of data is a big problem faced by the service providers. The distribution of data, synchronized of data at server and receiver side and security is effect the overall system.

In fact, the cloud architecture faced a lot of challenges while performing any transaction. But security of data is main concern. The personal data on cloud should be secure from unauthorized access, should be save from internal and external attacks, and must be store for long time for future use.

V. CONCLUSION

E-governance and Cloud both take initiatives to provide the services to clients at less cost, more transparent, accurate and in secure environment. The public use the online services of the government, if these services provide on cloud it become more beneficial for citizens. They take the advantage from virtual environment provided by the cloud and save time and money. The required software, hardware, platform and infrastructure all these access from cloud and pay only for what they used. The user need not purchase their own, the existing resources provide them on demand basis. The cloud based E-governance may be having some challenges but these challenges would not criticize the architecture of cloud. It would seem to be a secure and reliable environment for the citizens. It encourages the user to share and access the resources on cloud based framework of E-governance.

VI. REFERENCES

- [1]. Suchitra Pyarelal (2004), Interoperability Framework for E-Governance (IFEG): Strategic Approach to Evolve National Standards. Informatics.
- [2]. Gupta, M., P., Jana, D., (2003), E-government evaluation: A framework and case study, Government Information Quarterly 20.
- [3]. Gupta, M. P., Kumar, P. and Bhattacharya, J., (2005), Government Online: Opportunities and Challenges, Tata McGraw-Hill Publishing Company Limited.
- [4]. Bhatnagar, S., Rao, T. P., Singh, N.,Vaidya, R., Mandal, M., (2007), Impact Assessment Study of E-government Projects in India.
- [5]. S.K. shrivastava, A.N. Pandey, P.Kumar, Interoperability issues for E-Governance Framework.
- [6]. Dr. Nityesh Bhatt, e-Governance Frameworks: Agenda Ahead, Reseek.
- [7]. A.D.Pairkh (2010), Software Design Pattern For E-governance Solution Framework.
- [8]. J.Hackler and J P.Holdren (2008)“Walking The Talk And Walking The Walk At The Woods Hole Research Center”, Journal of Green Building, Volume 3.

- [9]. Sanderson, George F. (1992), “Climate change: the threat to human health”, The Futurist.
- [10].H. Singh (2012), Technology transfer model to migrate e-governance to cloud computing, IJATER, volume 2 Issue 4.
- [11].Geoffrey R. K. (2012), A Framework for Securing e-Government Services: the case of Tanzania.
- [12].V.J. Singh, A. Chandel (2014), Evolving E-Governance through Cloud Computing based environment, IJARCCCE, Vol 3, Issue 4.
- [13].T. Kajiyama (2012), Cloud computing security: how risks and threats are affecting cloud adoption decisions.