Analysis of Cloud Computing Security Framework in E-governance

[1]Sapanjeet Kaur, [2]Dr. Dinesh Kumar
[1]Research Scholar, Guru Kashi University, Talwandi Sabo, Punjab, India
[2]Associate Professor, Guru Kashi University, Talwandi Sabo, Punjab, India

Abstract

The concept of cloud computing becomes important for each government, facilitating its way of work, increasing its productivity and all that leading to cost savings. Different country chooses different strategy for adoption of cloud computing with a possibility to become better and more effective e-government.The aim of the present paper is to study the services of cloud computing in e-governance, challenges in implementing and various security issues and methodology to prevent the threats of data.

Keywords

Cloud computing, Security Issues, E-Governance, Trust Based Protocols.

I. Introduction

E-Government provides a paper free environment and improve the structure for delivering information and services to users by using Information and Communication Technology (ICT). The services of E-governance have grown rapidly from past few years. The consumption of hardware and software is increased and the user wants to get maximum benefits from these resources. Some companies take initiatives to reduce cost and better utilizing of existing resources. Cloud computing is the new technology for find the solution of these challenges. The unique characteristics of cloud computing has turned the environment of E-governance more valuable and effective. The complexity and expansion of E-government is being observed, so the size of computational data is increased day by day. It is a model that helps to implement the services of E-government more satisfactory and efficiently to the service user of the cloud. Through cloud computing the high computational problems can be solved easily and in appropriate manner. This technology is used to identify the development of services and use in E-governance architecture and tried to overcome the weakness of service delivery. The other benefits of the cloud computing in E-government are cost reduction, integration and reusability of services can be noted [1].

II. Cloud Computing in E-governance

Cloud computing is an emerging technology to deliver flexible, cost effective and secure services to the users over the internet. The importance of cloud computing is cumulativeand also mounting attention in different departments of E-governance. It is seeing in the top most technologies in different organization. Cloud computing is on demand network access to share the resources (e.g. networks, servers, storage, applications, and services) to satisfy the need of user [2].

Cloud computing is constructedfor transferring databases and services at lower cost. But security is the major difficulty beside it. The security issues are considered at the both ends of service delivery. These services hosted by the clouds and security issues are categories among cloud service user and cloud service provider [3]. The another study listed the parameters that affect the security of cloud then it explores the cloud security issues and problems faced by the cloud provider and the cloud consumer such as data, privacy, and infected application and security issues [4]. Headayetullah et al (2010) proposed an innovative and proficient trust based security protocol in his study. This protocol assures for the sharing of top secret information of government intelligence agencies globally. There are various models of cloud computing and issues of data security. The complexity in cloud computing become obstacle to achieve end to end delivery. Another research work of Wang et al investigated the problem of data security in cloud data storage which is essentially a distributed storage system. It also discussed the integration of storage correctness insurance and data error localization.

III. Classification of Different Clouds

A. Public Cloud

The public cloud provides the resources, applications, and web based services to the users. It is for the public use and accessible to all public organizations.

B. Private Cloud

Private cloud is for the exclusive use and only for an organization, so everyone in the organization can access data, services and applications but others out of organization cannot access the data.

C. Community Cloud

Community clouds are designed to provide some common facilities and resources to the users. It can be shared between one or some organizations but the service users are follow the same policy and security and also demand for the same type of resources. The community clouds are used by the group of organizations working on same task.

D. Hybrid Cloud

The last cloud is Hybrid ones which are combination of two or more clouds. It is an environment which uses some internal and external cloud users.

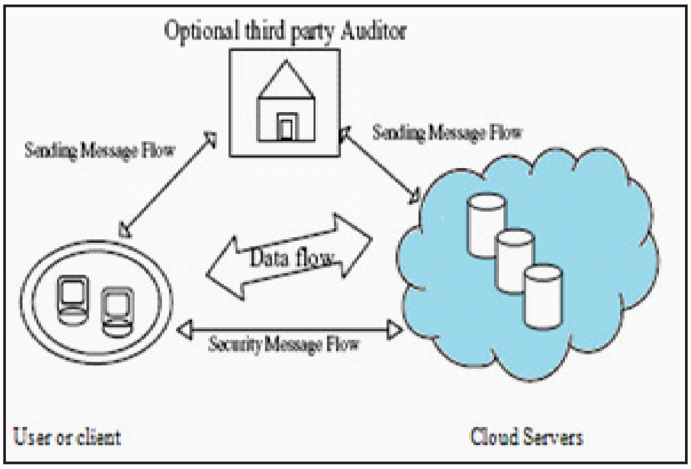

Fig. 1: Data Flow of Cloud Architecture

The figure illustrates the technical details of providing the services to the cloud users and the arrangement of cloud service provider's network. Security is also a main issue in the cloud environment.

IV. Services Provided by Different Layer of Cloud Computing

A. Software as a Service (SaaS)

It is used to access the applications running on the cloud infrastructure by the cloud users e.g. wed based mails.

B. Platform as a Service (PaaS)

It refers to providing platform layer resources, including operating system and software development frameworks that can be used to build higher-level services.

C. Infrastructure as a Service (IaaS)

It is the provision of 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 other applications.

V. Framework of Cloud Computing Environment

The cloud environment provide the demand based services to the cloud users and establish a secure and reliable environment to the users as well as the service providers.

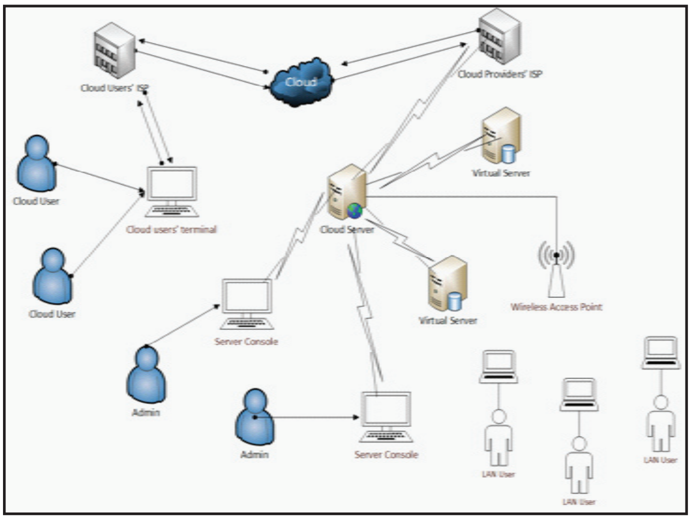

Fig. 2: Framework of Cloud Environment

The basic design of cloud computing is defining in fig. 2. All the characteristics of clouds like accessibility of cloud, cloud provider architecture, identification of cloud users and flow of request and service providing. It describes the basic design of providing services to the cloud service users by the cloud service provider. The cloud service provider performs the service on demand basis. Some LAN users also access the resources of cloud but they do not use the requested resource all the time. Cloud admin is only identifying the cloud users by their remote location. TheLAN users consider as the cloud service users when they use the services offered by the servers. They just borrow the resources from the servers on demand basis.

VI. Challenges of Service Delivery in Cloud Computing

Cloud computing is used the facility of internet to sharing the internet infrastructure and allow to communicate between client side and server side. But thesecurity is the major issue in cloud environment at both ends i.e. cloud service user and cloud service provider. The security is necessary at all level such as data storage, network environment, hosts and application software. There is dependencies and relationships between services of the cloud based model such as PaaS, SaaS and IaaS. PaaS offers a platform to build and deploy SaaS applications, which increase the security dependency between services. The dependability and security are distinct but having convergent paths: dependency restrict to appearance the fault not in whole system but will be occur only at a particular part of the system. Security is always providing the confidentiality and integrity in provided data.The security is essential for the cloud environment where the same resources are shared by the different users. The different security attacks are defined while sharing data and resources. Some major security threats are discovering in cloud computing [5]:

A. Insecure Application Programming Interfaces

Due to the sharable environment the different cloud users access the same resources and software. In this environment of clouds, the applications are not secure and access by the unauthorized parties.

B. Unbearable Insiders

The service provider are not always faithful they use the environment for person benefits and leak the secret information.

C. Shared Technology Weaknesses

The sharing clouds infrastructure is also weak point. The data is open for all the service users but not sure everyone is reliable or not.

D. Data Loss

In the networking environment the virus and worms are well known threat. These are the piece of code that effects the hardware and corrupt the files.

E. Repudiation

Repudiation is another issue in which the sender denial the validity of any statement or service.

F. Tampering

Tampering is an attack which occur when the attacker amends some information in stored files or shared files.

G. Information Disclosure or Eavesdropping

The attacker hijack the path of any databases or file and access the information for person benefits and spoil the transmission.

H. Replay Attack

It is defined when the hijacker sends a valid data having fraud intension. An attacker access the unauthorized information is called Elevation of Privileges.

I. Man in the Middle Attack

It happens when attack infiltrate the transmission media and take authority forcefully to transfer data and modify the files.

J. Identity Spoofing

It occurs when the attacker bluffs the user as the originator of the message to take the advantage of network media [5].

The various methods are developed to find the security risks and find out the appropriate solution for all these threats.The most fundamental problem facing by the organizations who want to protect their data from theft and unauthorized access. In distributed environment the databases, resources and software are shared frequently and corresponding risks are there for data.

VII. Security Issues and Solutions to provide Secure Environment

An investigation the possibility of the data/information being secure in the cloud computing environment. The cloud security issues and their solutions are:

A. Single Sign In

The users of cloud will have multiple logins but thiswill lead to authentication problems, so strongauthentication at user level should be provided within thecloud.

B. Cloud Secure Federation

This problem occurs when cloud consumer controls applications that depend on the services provided by different clouds, it needs to maintain its security on both clouds and in the transmission. This problem can be overcome by identity federation, single sign on, authentication and permission can help to solve security issues.

C. Availability of Information

When an organization implement its process, services and applications to cloud they take an assumed risk in terms of non-availability of data when they need it most. The way to mitigate the unavailability of data and resources is to have backup plan to cover an outage event also for local resources for central information. The provider should provision aobserving and report system that permit the consumers know about the data atprobable time.

D. Third Party Control

The cloud service provider has no control on their own data and the processing of the resources and data as this is a third party issue. Cloud providers are not aware about the architecture of Cloud and the proper security is not provided to the cloud users. Sometimes user can be locked with one vendor. This happens because of contract or hard to migratethe data from old to new vendor.

E. Information Integrity and Privacy

The resources in the clouds are valid to users as well as attackers. A boarder's resources can be accessed through web browsers, remote connections and from personal computers too. The information security privacy and authentication issues are absence of verification, permission and secretarial controls and no management of encryption and decryption keys.This problem is solved by providing proper authentication, access control. So anyone want to access the information goes through different type of checking to ensure only authorized persons access the information and resources.

F. Secure Information Management

The cloud management can be extended to include and organizecomponents such as service observing, billing, servicesarchive and security management of the cloud. Thisis very serious when any holeoccursin the service of this layer. The hackers or unauthorized persons having control like anadministrator, over the whole cloud network. The solutionfor this is to include security requirements and policiesspecifications derived from occupant organizations which arerevised and realistic in occupant 'sphysical environment, andfeedback from environment to security management and cloud user.

G. Integrity of Information

The integrity is achieved when there is a mutual faith between the cloud service providers and cloud service users and they complement of each other and support the security such that whole system works faultlessly. To achieve this proper authentication, Authorization and accounting controls should be implemented by the cloud service provider and the users.

H. Repudiation of Information

The consumer and the provider find themselves in a deep hole when it comes to prove the transaction they did was indeed them, or may decline that it was them. To prevent this issue at cloud level, cloud provider has to ensure that non-repudiation enabled protocol or handshake is deployed whereby, the engaging parties cannot dismiss their participation in argued transaction [10].

I. Security Management

The security management in cloud hang on two parts: what security controls must the customer provide over and above the controls inherent in the cloud platform and how must an organization 's security in the cloud. Both of these factors must be continually reevaluated based on the sensitivity of the data and the service-level changes over time.

VIII. Conclusion

Although cloud computing has a potential for governmental adoption, issues and challenges of governmental cloud computing still remain in some parts. The advantages of cloud computing also very helpful to be adopted in the public sector and e-Government. In this paper, we provide Cloud Security issues in terms of Cloud Service users and providers and also define the solution to tackle these problems while sharing data and resources in cloud environment. The management of security at all levels of transmission is must. So thefurther research is required in the field of data security.

References

[1] S. Hashemi, K. Monfaredi, M. Masdari,"Using Cloud Computing for E-Government: Challenges and Benefits", IJCEACIE, Vol. 7, No. 9, 2013.

[2] K.Hashizume, D. G Rosado, E. Femandez-Medina, E. B Fermandez,"An Analysis of security issues for Cloud Computing", JISA, 2013.

[3] K. Lee,"Security Threats in Cloud Computing Environments", International Journal of security and its applications, Vol. 6, No. 4, October 2012.

[4] P. Jain,"Security Issues and their Solution in Cloud Computing", International journal of Computing and Business Research, proceeding of 'I- Society 2012', 2012.

[5] A. Malik, M. M. Nazir,"Security Framework for Cloud Computing Environment: A Review", JETCIS, Vol. 3, No. 3, March 2012.

[6] Md. Headayetullah, G.K. Pardhan,"Interoperability, Trust based information sharing Protocol and Security: Digital Government key issues", IJCSIT, Vol. 2, No. 3, June 2010.

[7] Nalini, Manivannan, Vaishnavi,"Efficient Remote Data Possession Checking in Critical Information Infrastructures ensuring Data Storage Security in Cloud Computing",

IJIRCCE Vol. 1, Issue 1, 2013.

[8] M.Ahmed, M.A.Hossain,"Cloud Computing and Security Issues in the Cloud", IJNSA, Vol. 6, No. 1, January 2014.

[9] R.P. Padhy, M.R. Patra, S.C. Satapathy,"Cloud Computing: Security Issues and Research Challenges", IJCSITS, Vol. 1, No. 2, December 2011.

[10] C Wang, Q Wang, K Ren, W Lou,"Ensuring Data Storage Security in Cloud Computing", US National Science Foundation under grant CNS-0831963, CNS-0626601.

[11] Manas M., Nagalakshmi c., Shobha G.,"Cloud Computing Security Issues and Methods to Overcome", IJARCCE, Vol. 3, Issue 4, April 2014.

[12] AkhilBehl, KanikaBehl,"Security Paradigms for Cloud Computing", Fourth International Conference on Computational Intelligence, Communication Systems and Networks, IEEE, 2012.

[13] MeikoJensen, JorgSehwenk,"On Technical Security Issues in cloud Computing", IEEE International conference on cloud Computing, 2009.

[14] AkhilBehl, KanikaBehl,"An analysis of cloud computing security issues", World Congress on Information and Communication Technologies, IEEE, 2012.