

Cloud Computing and Data Security Challenges: A Nepal Case

Shailendra Giri^{#1}

[#]Executive Director, Personnel Training Academy
Ministry of Federal Affairs and General Administration
Kathmandu, Nepal

Abstract

Cloud computing is being an alternate choice of computer and mobile users for the data storage and access. Cloud computing and data security both are being major issues in Nepal. The author is trying to explore about cloud computing and data security in cloud. The content analysis method is used to conduct the study. The study concludes that the cloud computing is essential for Nepal means of data accessible, regulation and storage. Nepal is under developed country as well it has not sufficient technological knowhow, sufficient financial resources, huge digital divide, and skilled human resources so the data security issue is genuine in this time. The storage, virtualization, and networks are the major security concerns in Cloud Computing. Virtualization allows multiple users to share a physical server is one of the key concerns for cloud users and providers. Cloud networks are in target for attacks particularly while communicating with remote virtual equipment basically their target in data. It is clear that Nepal is facing many challenges in cloud computing are securities, storage, data centre operation, costing model, charging model, service level agreement, locality, integrity, access, segregation, breaches and confidentiality. Nepal is one of the developing country, it should start to use own sever and satellite for communication as well as data centre or data bank.

Keywords - Cloud computing, data security challenges, security model, vulnerabilities, e-government.

I. INTRODUCTION

Cloud computing is fast growing and accepted computing model for hosting large computing systems and services [19]. According to Gartner [20] measured Cloud Computing as the first among the top 10 most important technologies. It is changing the way and operational expenses in information and communication technology (ICT) and has changed the way infrastructures and reform current computing age. Cloud computing has also massively removed start-up Costs for new companies and has influenced how we store and process data [17]. The use of cloud computing is covering large scope, floppy disk, hard disk, CD, USP, were used as mass storage but at present everyone loves cloud computing. Big organization as well as individuals uses it like a tool,

as a mean of file and data sharing. Being fundamental assets, it has been making file and resource sharing easy and fast. Using the internet and virtual space software; people could store their important data, secret information on it.

It permits firms to avoid or minimize up-front IT infrastructure prices and permits enterprises to urge their applications up and running more rapidly, with improved flexibility and less maintenance, which it permits IT groups to faster regulate resources to satisfy unsteady and unpredictable demand[20],[3],[13]. The provision of high-capacity networks, affordable computers and storage devices still because the widespread adoption of hardware virtualization, service-oriented design, and involuntary and utility computing has crystal rectifier to growth in cloud computing [5]. In cloud computing environments, data is the fundamental asset that we need to secure [17]. It is no need to carry mass storage devices like hard disk, floppy disk, CD, memory card, USB and so on. We can easily retrieved our file easily from anywhere of the world due to data are store on the cloud. Hard disk, floppy disk, CD, USB have limited storage capacity so, cloud computing has been using. Cloud computing provides 5 Gb free space to the user. If they need more space, they should buy as they need.

The importance of Cloud Computing is increasing and receiving a growing attention in the scientific and industrial community. Cloud Computing is obtainable anywhere, suitable, on-demand network access to a shared pool of configurable computing resources. Cloud Computing seems as a computational paradigm as well as a distribution structural design and its main aim is to provide secure, fast, suitable data storage and net computing service, with all computing resources visualized as services and delivered over the Internet [3],[21]. The cloud permit collaboration, agility, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work. It provides potential for cost reduction through optimized and efficient computing [10]. There is rapid increase in communication and data storage in cloud and its security in the last few years. Still there are many difficult and computation rigorous problems in data security in cloud computing [4].

IT is becoming a worldwide cloud increasingly embedding the computational and storage resources

that are able to meet the requirements of emerging applications [16]. The constant developments of technology in computing and networks, the virtualization capabilities allow a new approach. [8]. Cloud computing proposes to rework the manner it's consumed and managed with guarantees of improved price efficiencies, accelerated innovation, quicker time-to-market, and therefore the ability to scale applications on demand [29]. It helps to meet the emerging demands of open innovation and flexibility required for global service platforms [28]. The main principle of cloud computing is compute, storage, and Software as a Service, (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), or as a utility, Data as a Service (Daas) [4].

The objective of this study is to secure data in cloud computing. This article provides a detailed description of data security in cloud computing. The article will further analyze how data could be made secure in cloud in case of Nepal. Types of cloud, cloud computing service models, data security and issues in cloud computing, data security challenges in cloud computing and vulnerabilities in cloud computing are studied on this piece of writing.

II. LITERATURE REVIEW

As a metaphor for the Internet the term cloud has been used historically. This concept dates back as early as 1961, when Professor John McCarthy suggested that computer time-sharing technology might lead to a future. This idea became very popular in the late 1960s. It became clear that the IT-related technologies of the day were unable to sustain such a artistic movement computing model. The mid-1970s this idea became out of date. The term cloud computing began to emerge in technology circles during this time [13]. The vision of using and sharing computers and data as utility has been inspired by constantly increasing computing needs faced by researchers in science and can be traced back in the 1960s to the Internet. Different names are used for this kind of platform, including utility computing, on-demand platform, and platform as a service [18].

Cloud computing is the dynamic delivery of information technology resources and capabilities as a service over the Internet. According to Gartner Group [30], the attributes of cloud computing are service-based, scalable and elastic shared, metered by use, use of Internet technologies. The advantages of cloud computing are, it is agile, with ease and speed of deployment, its cost is use-based, and will likely be reduced, in-house IT costs are reduced, capital investment is reduced, the latest technology is always delivered, the use of standard technology is encouraged and facilitated [7], [30].

One of the most popular ones is from the National Institute of Standard and Technology (NIST), which defines cloud computing as follows. "*Cloud computing is a model for enabling ubiquitous,*

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" [20].

All cloud computing approaches are not the same, and several deployment models, while different, are still considered clouds computing are [14]:

Private cloud: The cloud infrastructure is owned or leased by a single organization and is operated only for that organization.

Community cloud: The cloud infrastructure is shared by several organizations and supports fix community that has shared concerns.

Public cloud: The cloud infrastructure is owned by an organization selling cloud services to the general public or to a large industry group.

Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (internal, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

A. Cloud Computing Service Models

According to the NIST [20] definition, cloud computing services can be classified based on the service model they use to create the services. There are three cloud computing service models. They are:

1. Infrastructure as a Service (IaaS)

The services, provided in this model, allow the cloud user to interact directly with the hardware resources. The consumer is provided the capability to provision, computing power, storage and network resources. The consumer also has the responsibility of supplying software to run on the hardware resources, which can include operating systems and application software. As a result, although the user does not manage the underlying cloud resources, it has control over operating systems security and application security while having limited control over network security [20].

2. Platform as a Service (PaaS)

In the PaaS model, the user is provided with a development environment with tools, services and libraries. The user can create cloud services using the provided environment while bounded by the limitations of the environment. In this service model, the user has control over the applications/services which it creates but not the underlying hardware or software.

3. Software as a Service (SaaS)

The SaaS model provides software to a cloud user that it may need. It frees the user from resource maintenance to a large extent while providing the required functionality. This model offers the least

amount of control to the user. It may provide customizability of the software to fit the user's need but no control over the software, the platform or the infrastructure.

The ISO standard ISO/IEC 1728 identifies these service models as cloud capabilities and defines seven cloud service categories [17] are CaaS: Communications as a Service, CompaaS: Compute as a Service, DSaaS: Data Storage as a Service, IaaS: Infrastructure as a Service, NaaS: Network as a Service, PaaS: Platform as a Service, SaaS: Software as a Service.

B. Data Security and Security Issues in Cloud Computing

Cloud computing is a new model of resource sharing. Many of us are already using cloud computing in our daily lives for personal use [25]. Data security is a common concern for any technology now. It is becoming a major challenge when SaaS users have to rely on their providers for proper security [24],[26], [27]. The main ambition of Security is to limit access only to those approved, to let those with approved see and/or modify only the data they are entitled to see and no other data, and to ensure that no one can demand resources [25]. When entrusting an organization's critical information to geographically dispersed cloud platforms not under the direct control of that organization the principal concern is security.

Data backup is a serious task to store and maintain its security order to facilitate recovery in case of disaster [26]. Now its attention about cloud computing environments and describes the methodology for guarantee about data security. The major concern is how cloud resources should be protected in the Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) environments and offers security best practices for service providers [23].

In SaaS, organizational data is often processed in plaintext and stored in the cloud for the further access. The SaaS provider is the one responsible for the security of the data in the cloud. When it is being processed and stored on the cloud [15]. Today, users of cloud computing are looking toward horizons to expand their on-premises infrastructure and cannot afford the risk of compromising the security of their applications and data. Security of data is greatest challenge or issue of cloud computing [12]. Cloud providers preserve subcontract other services such as backup from third-party service providers. [24].

C. Data Security Challenges in Cloud Computing

1. Security

It is known that the security issue has played a key role in hindering cloud computing. The multi tenancy model and the pooled computing resources in

cloud computing has introduced security challenges [31].

2. Storage

The data stored in virtual machines have many issues one such issue is reliability of data storage. Virtual machines needs to be stored in a physical infrastructure which may cause security risk.

3. Data Center Operation

In case of data transfer bottlenecks and disaster, organizations using cloud computing applications needs to protect the user's data without any loss. If data is not managed properly, then there is an issue of data storage and data access. In case of disaster, the cloud providers are responsible for the loss of data

4. Costing Model

During migrating to the cloud can significantly reduce the infrastructure cost, it does raise the cost of data communication. The cost of data integration can be substantial as different clouds often use proprietary protocols and interfaces. This requires the cloud consumer to interact with various clouds using cloud provider-specific. The splitting and mixing data not only adds substantial extra financial cost, but can also severely affect the system performance [1]

5. Charging Model

This include re-design and re-development of the software that was originally used for single-tenancy, cost of providing new features that allow for intensive customization, performance and security enhancement for concurrent user access, and dealing with complexities induced by the above changes.

6. Service Level Agreement

Although cloud consumers do not have control over the underlying computing resources, they do need to ensure the quality, availability, reliability, and performance of these resources when consumers have migrated their core business functions onto their entrusted cloud. In other words, it is vital for consumers to obtain guarantees from providers on service delivery. In addition, different cloud offerings (IaaS, PaaS, SaaS, and DaaS) will need to define different SLA meta specifications.

7. What to migrate

At present, peripheral functions such as IT management and personal applications are the easiest IT systems to move. Organizations are traditional in employing IaaS compared to SaaS. This is partly because marginal functions are often outsourced to the Cloud, and core activities are kept in-house.

8. Locality

In cloud computing, the facts is distributed over the wide variety of areas and to discover the region of information is difficult. when the statistics is moved

to special geographic locations the legal guidelines governing on that data also can trade. So there may be an issue of compliance and statistics privacy legal guidelines in cloud computing. customers need to know their facts vicinity and it's far to be intimidated through the service provider.

9. Integrity

The system must preserve security such that statistics may be only changed by way of the authorized man or woman. In cloud primarily based surroundings, facts integrity need to be maintained efficaciously to keep away from the statistics misplaced. In preferred each transactions in cloud computing should follow ACID houses to preserve statistics integrity. most of the internet offerings face lot of issues with the transaction management regularly because it makes use of HTTP offerings. HTTP carrier does no longer aid transaction or assure transport. it can be dealt with by enforcing transaction control inside the API itself.

10. Access

Data access mainly refers to the data security policies. In an organization, the employees will be given access to the section of data based on their company security policies. The same data cannot be accessed by the other employee working in the same organization. Various encryption techniques and key management mechanisms are used to ensure that data are shared only with the valid users. The key is distributed only to the authorized parties using various key distribution mechanisms. To secure the data from the unauthorized users the data security policies must be strictly followed. Since access is given through the internet for all cloud users, it is necessary to provide privileged user access. User can use data encryption and protection mechanisms to avoid security risk.

11. Confidentiality

Data is stored on remote servers by the cloud users and content such as data, videos etc., can be stored with the single or multi cloud providers. When data is stored in the remote server, data confidentiality is one of the important requirements. To maintain confidentiality data understanding and its classification, users should be aware of which data is stored in cloud and its accessibility.

12. Breaches

Data Breaches is another important security issue to be concentrated in cloud. Since large data from various users are stored in the cloud, there is a possibility of malicious user entering the cloud such that the entire cloud environment is prone to a high value attack. A breach can occur due to various accidental transmission issues or due to insider attack.

13. Segregation

One the major characteristics of cloud computing is multi-tenancy. Since multi-tenancy allows to store data by multiple users on cloud servers there is a possibility of data intrusion. By injecting a client code or by using any application, data can be intruded. So there is a necessity to store data separately from the remaining customer's data. Vulnerabilities with data segregation can be detected or found out using the tests such as SQL injection Data validation and insecure storage.

D. Vulnerabilities in Cloud Computing

Mainly, we focus on technology-based vulnerabilities but there are other vulnerabilities in all organization. Some of these vulnerabilities are:

Lack of employee screening and poor hiring practices [6]– some cloud providers might not perform background screening of their employees. Private users such as cloud administrators usually have unlimited access to the cloud data.

Lack of customer background checks– many of cloud providers does not check their customer's environment, and more or less anyone can open an account with a valid credit card and email [6].

Lack of security education– citizens continues to be a weak point in information safety [22]. This is true in any type of institute; though, in the cloud, it has a superior impact because there are many people that network with the cloud: cloud providers, third party providers, suppliers, organizational customers, and end-users.

Cloud Computing have been existing technologies such as web services, web browsers, and virtualization, which contributes to the evolution of cloud environments. So, any vulnerability associated to these technologies which affect the cloud, and it can even have a significant impact in data security in the cloud [11].

III.DISCUSSION

Cloud computing services contain extremely optimized virtualized data centres providing hardware, software and information resources for use, whenever they are required but data and information security challenge in cloud is big issue at present time. The more cloud systems are developed and new concepts are introduced while the cloud computing technology continues to emerge. Highly available cloud applications can be constructed, for example, by deploying them on two competitive cloud offerings, e.g., Google's App Engine [9] and Amazon's EC2 [2]. Cloud computing offers a massive pool of resources and services that cloud user's can utilize for storing and processing their data. Although cloud computing has many benefits as well as demerits too. Data security is one of the top concerns of data owners

when moving operations to the cloud. Most of these cloud specific issues arise due to the new attack vector. Encryption-decryption techniques have used for long time to secure important data. Digital signature and firewall could also protect data on cloud if maintained it properly. Government of Nepal also give concentration towards data security policy, act and plan in days to come. Government should start to develop own data bank in the country and integrated data store system should apply in government agencies and other concern stake holders at right time. Cyber attract, threat, hacking, cracking, high-jacking are increasing day by day. All of above focus on data.

IV.CONCLUSION

Cloud computing has become a fundamental part of the computing world. It provides IT services over the Internet where cloud user does not have knowledge about wherever the data or information is being stored and where the infrastructure is located. The cloud users receive services without knowing any of the details about how it's provided and from where. The countries' commitment to maintain security of the cloud is essential at present time. The safe cloud computing environments guarantee about data security in cloud computing. These models could be fit in case of Nepal for data protection in cloud is the Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). It is clear that Nepal is facing many challenges in cloud computing is security, storage, data center operation, costing model, charging model, service level agreement, locality, integrity, access, segregation, breaches and confidentiality. The study concludes that storage, virtualization, and networks are the major security concerns in Cloud Computing. Virtualization allows multiple users to share a physical server is one of the key concerns for cloud users and providers. The other challenges are different types of virtualization in technologies. Virtual networks are in target for attacks particularly while communicating with remote virtual equipment basically their target in data security. Nepal is one of the developing country, it should start to use own sever and satellite for communication and data centre.

REFERENCES

- [1] A.Leinwand, (2009)."The Hidden Cost of the Cloud: Bandwidth Charges," <http://gigaom.com/2009/07/17/the-hidden-cost-of-the-cloud-bandwidthcharges>
- [2] Amazon Elastic Compute Cloud. <http://aws.amazon.com/ec2/>
- [3] Baburajan, R. (2011). "The Rising Cloud Storage Market Opportunity Strengthens Vendors". <http://it.tmcnet.com>.
- [4] Bele, S. B (2018). A Comprehensive Study on Cloud Computing. International Journal of Information Research and Review. Vol. 05, Issue, 03, pp.5310-5313
- [5] Cloud Computing: Clash of the clouds", 2009. The Economist. www.economist.com.
- [6] Cloud Security Alliance (2010). Top Threats to Cloud Computing V1.0. Available: <https://cloudsecurityalliance.org/research/top-threats>
- [7] Conti, Marco, (2011)."Research challenges towards the Future Internet", Computer Communications, 34(18), 2115–2134
- [8] For a detailed analysis of NRENs in Europe and their role, see the documents (in particular the TERENA compendium), <http://www.terena.org/publications/>
- [9] Google App Engine. <http://code.google.com/appengine>. Retrieved : 9 February, 2019.
- [10] Grumman, G. (2008). What cloud computing really means". InfoWorld. Retrieved: 10 February, 2019.
- [11] Hashizume (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications .
- [12] <http://cloudsecurity.org/2008/10/14/biggest-cloud-challenge-security>, retrieved 29 Feb 2019.
- [13] <http://computinginthecloud.wordpress.com/2008/09/25/utility-cloud-computingflashbackto-1961-prof-john-mccarthy>, retrieved 5 Jan 2019.
- [14] <http://csrc.nist.gov/groups/SNS/cloud-computing/index.html>
- [15] Ju J, Wang Y, Fu J, Wu J, Lin Z (2010). Research on Key Technology in SaaS. In: International Conference on Intelligent Computing and Cognitive Informatics (ICICCI), Hangzhou, China. IEEE Computer Society, Washington, DC, USA, pp 384–387
- [16] Koslovski G., Huu T. T., Montagnat J., & Primet P. V.-B, 2009. First International Conference, CloudComp 2009. Munich, Germany, October 19-21.
- [17] Kumar., V., Chaisiri, S. ,Ko.R.(2017). Data Security in Cloud Computing. The Institution of Engineering and Technology. Published by The Institution of Engineering and Technology, London, United Kingdom.
- [18] Li Henry (2009). Introduction to Windows Azure An Introduction to Cloud Computing Using Microsoft Windows Azur. Printed and bound in the United States of (America Mustafa S.2015). Resource management in cloud computing: Taxonomy, prospects, and challenges. Computer Electrical Engineering, <http://dx.doi.org/10.1016/j>.
- [19] National Institute of Standards and Technology, (2011). The NIST definition of cloud computing; <http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf>
- [20] Oestreich, Ken, (2010). "Converged Infrastructure". CTO Forum. Thectoforum.com.
- [21] Popovic K, Hocenski Z. (2010). Cloud Computing Security issues and challenges. In: Proceedings of the 33rd International convention MIPRO. IEEE Computer Society Washington DC, USA, pp 344–349
- [22] Rittinghouse John W. & Ransom James F. (2010). Cloud Computing Implementation, Management, and Security. CRC Press Taylor & Francis Group. Boca Raton London- New York
- [23] Rittinghouse JW, Ransome JF (2009). Security in the Cloud. In: Cloud Computing. Implementation, Management, and Security, CRC Press
- [24] Sarana David E.Y. Implementing and Developing Cloud Computing Applications. CRC Press. Auerbach Publications Taylor & Francis Group. USA
- [25] Subashini S, Kavitha V. (2011). A survey on Security issues in service delivery models of Cloud Computing. Netw Comput Appl 34(1):1–11
- [26] Viega J.(2009) Cloud Computing and the common Man. Computer 42(8):106–108
- [27] Villasante Jesus (2009). Cloud Computing Enabling the Future Internet. First International Conference, CloudComp 2009. Munich, Germany, October 19-21.
- [28] Walther Dane S.(2009). Akamai and Cloud Computing. First International Conference, CloudComp 2009. Munich, Germany, October 19-21.
- [29] www.gartner.com/technology/initiatives/cloud-computing.jsp.
- [30] Y. Chen, V. Paxson, and R. Katz, (2010). "What's New About Cloud Computing Security?"