Cloud Computing and Data Security Challenges: A Nepal Case

Birendra Prasad Yadav

Faculty of Tribhuvan University, Nepal (TRMC)

Abstract

When it comes to storing and accessing data, cloud computing provides an alternative option for users of computers and mobile devices. Nepal has a lot of problems with cloud computing and protecting data. Data security in the cloud and cloud computing are topics the author is investigating. The investigation is carried out using the content analysis method. According to the research, cloud computing is crucial for the storage, regulation, and accessibility of data in Nepal. Additionally, Nepal is a developing nation. The data security issue is real because it has lacked the necessary technological know-how, financial resources, human resources with the necessary skills, and a large digital divide. Security in the cloud is mostly concerned with storage, virtualization, and networks. Users and providers of cloud services are primarily concerned in virtualization, which enables numerous users to share a single physical server. Data transmitted by remote virtual equipment is a prime target for assaults on cloud networks. Security, storage, data center operations, pricing, service level agreement, location, integrity, access, segregation, breaches, and confidentiality are just a few of the cloud computing issues that Nepal is clearly encountering. Nepal, like many other developing nations, should begin to make use of its own servers, satellites, and data centers or banks for communication and storage.

Keywords

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

Introduction

Hosting massive computer systems and services in the cloud is a rapidly expanding and widely used computing paradigm [19]. Cloud computing was ranked #1 among the top ten most significant technologies by Gartner [20]. It is altering the manner in which infrastructures modify the modern computer era and is changing the operational expenditures of information and communication technology (ICT). In addition to changing the way we store and process data, cloud computing has greatly reduced the start-up costs for new businesses [17]. Cloud computing has several applications; traditional mass storage media such as floppy discs, hard drives, CDs, and USBs are no longer popular. Both large corporations and individuals use it as a medium for exchanging files and data. Thanks to these essential elements, sharing files and resources is now quick and straightforward. People might keep sensitive information safe by using the internet and software that allows them to enter virtual spaces. Enterprises are able to get their applications up and running faster, with more flexibility and less maintenance, which helps IT groups faster regulate resources to meet unpredictable and unsteady demand [20], [3], [13]. This, in turn, allows firms to avoid or minimize up-front IT infrastructure prices. As a result of service-oriented architecture, involuntary and utility computing, and the broad use of hardware virtualization, cloud computing has grown, allowing for the deployment of inexpensive processors, storage devices, and high-capacity networks [5]. We need to protect data since it is our most valuable asset [17]. No need to lug along bulky storage media like CDs, memory cards, hard drives, floppy discs, etc. Data saved in the cloud allows us easy file retrieval from any location in the globe. Due to the limited storage capacity of hard discs, floppy discs, CDs, and USB drives, cloud computing has become more popular. When using cloud computing, users are given 5 GB of free space. They should just purchase more room when they need it.

The scientific and business communities are beginning to recognise the rising significance of cloud computing. connection to a shared pool of programmable computer resources may be had anywhere with sufficient, on-demand network connection. This is known as cloud computing. It would seem that cloud computing is both a distribution structural architecture and a computational paradigm. Its primary objective is to provide a net computing service that is safe, quick, and appropriate for storing and processing data, with all computer resources seen as services and provided over the internet [3], [21]. Accelerating development work, facilitating collaboration, scalability, availability, and adaptability to demand changes are all made possible by the cloud. It offers the chance to save money by making computing more efficient and streamlined. The number ten. Cloud computing, including its storage, communication, and security features, has grown substantially in recent years. Data security in the cloud still presents a number of challenging and demanding computational issues [4]. IT is evolving into a global cloud, with storage and processing resources embedded more and more to fulfil the needs of new applications [16]. Virtualization enables a fresh strategy, which is in line with the ever-evolving state of computer and networking technologies. [8]. In order to reimagine its use and management, cloud computing promises better cost efficiency, faster innovation, shorter time-to-market, and, therefore, the capacity to grow applications on-demand [29]. It is useful for accommodating the ever-changing needs of worldwide service platforms and the rising tide of open innovation [28]. Data as a Service (DaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are the four cornerstones of cloud computing [4]. Data security in the cloud is the focus of this research. Information safety in the cloud is defined in depth in this article. Using Nepal as an example, the post will go into additional detail on how to make data safe in the cloud. Cloud computing service models, cloud computing kinds, cloud computing data security concerns, cloud computing data security problems, and cloud computing vulnerabilities are all covered in this piece of literature.

Literature Review

Historically, the term "cloud" has been used to represent the internet. Professor John McCarthy first proposed the idea that computer time-sharing technology would pave the way to a better future in 1961. In the late '60s, this concept exploded in popularity. It soon became apparent that the then-current state of information technology could not support such an artistic movement computer paradigm. This concept was considered dated by the mid-1970s. The concept of cloud computing first surfaced in the computer community around this period [13]. The ever-increasing computing demands encountered by scientific researchers in the 1960s gave rise to the idea of using and sharing data and computers as a utility, which has its roots in the advent of the internet. Utilities computing, on-demand platform, and platform as a service are among of the terms used to describe this platform [18]. computer in the cloud refers to the on-demand provisioning of computer resources and services by means of the internet. The characteristics of cloud computing, as stated by Gartner Group [30], include being servicebased, scalable and elastic, shared, and metered by usage, and using Internet technology. The benefits of cloud computing include its scalability, ease of deployment, cost-effectiveness, reduced capital investment, constant delivery of cutting-edge technology, and promotion and facilitation of the use of industry-standard technologies [7], [30].

The National Institute of Standards and Technology (NIST) has produced a popular one that describes cloud computing. "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]. Although many deployment patterns are distinct, they are all still categorized as cloud computing. many cloud computing methodologies [14] here: A private cloud is one in which just one company owns or leases the necessary hardware and software to run its cloud operations. The term "community cloud" refers to an online environment where several organisations pool resources in order to address common issues. An organisation that offers cloud services to the public or a big industry group owns the cloud infrastructure in a public cloud. In a hybrid cloud, data and applications may be moved from one cloud to another using standardized or proprietary technologies. Each cloud in the architecture can be either an internal, community, or public cloud, but they are all still separate and distinct.

Section A. Models for Cloud Computing Services One way to categories cloud computing services is by the service model they employ, as stated in the NIST [20] definition. There are three distinct models for cloud computing services. Here they are: 1. SaaS for Infrastructure This model's services make it possible for cloud users to communicate with hardware resources directly. The capacity to supply storage, processing power, and network resources is made available to the consumer. The onus for providing the operating systems and application software needed to run on the hardware resources also falls on the consumer. Therefore, while the user does not have direct control over the cloud's fundamental resources, it does have some say over the safety of its operating system and its applications, but not its network [20]. 2 PaaS stands for "platform as a service." The platform as a service (PaaS) paradigm ensures that users have access to development resources such as libraries, services, and tools. The user is able to build cloud services within the constraints of the given environment. The user under this service model is in charge of the apps and services it generates, but not the software or hardware that powers them. 3. SaaS–Software as a Service Software as a service (SaaS) models allow cloud users to get software as needed. Although it provides the necessary functionality, it greatly reduces the amount of work that the user has to put into maintaining the resources. Users have the least level of control with this model. There is no command over the program, platform, or infrastructure, but it does allow users to tailor the product to their needs. These service types are recognized as cloud capabilities by the ISO standard ISO/IEC 1728. Communications as a Service (CaaS), Compute as a Service (CompaaS), Data Storage as a Service (DSaaS), Infrastructure as a Service (IaaS), Network as a Service (NaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are the seven types of cloud services that are defined by it [17].

B. Protecting Data and Addressing Security Concerns in the Cloud —One novel approach to sharing resources is cloud computing. Cloud computing is already a common part of many people's everyday life [25]. Nowadays, the safety of user data is an issue for any technological system. When software as a service (SaaS) customers are dependent on their suppliers to ensure adequate security, it poses a serious problem [24], [26], [27]. The primary goal of security is to prevent unauthorized individuals from gaining access, to restrict authorized users to seeing and editing just the material that pertains to their job function, and to prevent resource demands [25]. The primary worry of committing a company's vital data to cloud platforms that are geographically scattered and not directly controlled by that company is security. Storing and protecting data in order to enable recovery in the event of a disaster is a major undertaking [26]. The focus has shifted to cloud computing settings, and the process for ensuring data security is described. The primary focus is on the best practices for safeguarding cloud resources in SaaS, PaaS, and IaaS frameworks and offerings. Security recommendations for those offering their services the number 23. Organisational data is frequently processed and stored in the cloud in unencrypted while using SaaS. Data security in the cloud is the responsibility of the SaaS provider. While it's in the cloud getting processed and saved [15]. Users of cloud computing nowadays are searching for new ways to extend their on-premises infrastructure; they simply cannot afford to take any chances with the safety of their data and applications. When it comes to cloud computing, data security is the biggest concern [12]. Cloud companies continue to rely on third-party service providers for additional services, such backup. [24].

C. Threats to Data Privacy in the Cloud 1. Safety, it's no secret that security concerns have been a major roadblock for cloud computing. Security issues have arisen as a result of cloud computing's multitenancy approach and its shared computing resources [31]. 2. Keeping Virtual machine data has various problems. Data storage reliability is one such issue. A potential security issue arises from the necessity of storing virtual computers in a physical infrastructure. 3. Function of the Data Centre In the event of data transport delays or natural disasters, businesses utilizing cloud computing must ensure that customer data remains intact. Data storage and access become problematic when incorrect data management occurs. Providers of cloud services are legally liable for any data lost as a result of a disaster. 4. A Model for Costing Data transmission costs will increase, but infrastructure costs may be drastically cut by moving to the cloud. Considering that many clouds frequently employ their own unique protocols and interfaces, the expense of integrating data might be considerable. To do this, they must use cloud provider-specific protocols when interacting with other clouds. Not only may data splitting and mixing result in significant additional financial costs, but it can also have a devastating effect on the performance of the system [1]. 5. Method of Charging The expenses associated with this include reworking the program from the ground up to accommodate several tenants, improving performance and security for users to use the system at once, and coping with the complications that arise as a result of all of the aforementioned modifications.6. Agreement on Service Levels After moving their critical business processes to the cloud, customers still have a responsibility to monitor the resources' availability, performance, dependability, and quality, even though they do not have direct control over them. Put simply, customers should insist on service delivery assurances from vendors. Also, each cloud services (IaaS, PaaS, SaaS, and DaaS) will have unique SLA meta requirements that they must describe.7. Things to move Information technology systems that handle peripheral duties, such IT administration and personal apps, are the most easily migrated. When compared to SaaS, organizations' use of IaaS is more conventional. This is due in part to the fact that core operations are typically retained in-house and peripheral tasks are outsourced to the cloud.8. Place The data in cloud computing is spread out over many different locations, making it impossible to pinpoint exactly where the data is stored. The regulations controlling the data might also change when the statistics are transferred to certain regions. As a result, cloud computing's compliance and statistical privacy regulations may be problematic. Customers should be informed about the location of their data by the service provider.8. Honesty In order to maintain security, the system must restrict data changes to authorized users only. To prevent data loss in a cloud-based environment, data integrity must be effectively maintained. Ideally, all cloud computing transactions would adhere to ACID standards in order to maintain the integrity of statistics. Transaction management is a common source of problems for most online products due to the utilisation of HTTP offerings. Neither transactions nor transit assurance are provided by HTTP providers anymore. The problem can be resolved by implementing API-level transaction control. 10. Entry Security policies for data are the most common type of data access. According to the company's security regulations, personnel will be granted access to the data portion. Even if two employees were working there, they would not have access to the same data. Encryption and key management systems guarantee that only authorized users may access the data. Several systems ensure that only authorized parties receive the key. Strict adherence to data security policies is necessary to protect data from unauthorized users. It is essential to grant privileged user access since all cloud users have access over the internet. To prevent security threats, users might employ data encryption and protection techniques. Eleven. Privacy Users of cloud services save information (including data, movies, etc.) on remote servers. It can be saved with one or more cloud service providers. Ensuring data confidentiality is a crucial need when storing data on a distant server. Users should be aware of what data is kept in the cloud and how to access it in order to keep data comprehension and classification discreet.12. Violations Concerns about data breaches are another critical area of cloud security. Because the cloud stores massive amounts of data from many users, it is possible for a malevolent user to get access to the cloud and launch a high-value attack on the whole cloud ecosystem. Accidental gearbox problems or insider assaults are two potential causes of a breach. Thirteen. Separation Cloud computing is characterized by its multi-tenancy feature. There is a risk of data infiltration due to multi-tenancy, which permits data storage by several users on cloud servers. Injecting client code or using any program might compromise data. Therefore, data must be stored independently of the rest of the customer's information. Tests like SQL injection, data validation, and insecure storage can identify or locate vulnerabilities with data segregation. Cloud Computing Security Flaws While much of our attention is focused on security holes in technology, every company has other potential weak spots. Here are a few of these weaknesses: Poor recruiting methods and a lack of background checks on staff members [6] it's possible that some cloud service providers don't check their workers' backgrounds. The data stored in the cloud is often accessible to private users (like administrators) without limits. Virtually anyone with an active credit card and an email address may sign up for a cloud account, and many providers don't even bother to look into their customers' environments before they approve them [6]. One area where information security is lacking is in the area of security education for the general public [22]. Although this is true in any institution, it is more effective in the cloud because to the large number of individuals who network with it, including suppliers, end-users, cloud providers, third-party providers, and Organisational customers. Technologies including web services, web browsers, and virtualization have all played a role in the development of cloud environments, and they have been known as cloud computing. Consequently, the cloud is susceptible to any security flaw in these technologies, and such flaws can have a major effect on the safety of data stored in the cloud [11].

Discussion

Virtualized data centers that provide cloud computing services are highly optimized and make available software, hardware, and data resources on demand. However, there are significant concerns over the security of data and information stored in the cloud. The evolution of cloud computing has coincided with the proliferation of cloud systems and the introduction of novel ideas. For instance, building and deploying on two competing cloud services, like Amazon Elastic Compute Cloud (EC2) and Google App Engine (GCP), can result in highly accessible cloud apps. Users of cloud computing have access to a vast array of resources and services for data storage and processing. Cloud computing offers several advantages, but it also has certain drawbacks. Data owners are understandably worried about the safety of their data when considering a move to the cloud. As a result of the new attack vector, most of these cloud-specific concerns occur. For quite some time, people have relied on encryption and decryption methods to protect sensitive information. When correctly managed, a firewall and digital signature can further safeguard data stored in the cloud. Data security policy, legislation, and future plans are also priorities for Nepal's government. It is imperative that the government initiates the development of the country's data bank and promptly implements an integrated data storage system for all relevant stakeholders. Hacking, high jacking, cracking, cyber attract, and threats are on the rise. The preceding is all data-centric.

Conclusion

Nowadays, cloud computing is an essential aspect of the computer industry. Customers of these cloud services are not privy to the physical location of the servers or data storage facilities, but rather receive IT support over the internet. Customers of cloud services are often in the dark about the origin and method of service delivery. At this time, it is critical that the nations pledge to keep the cloud secure. Protected cloud computing environments ensure the safety of data stored in the cloud. Software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) are three paradigms that can work for Nepal's data protection needs in the cloud. Security, storage, data center operations, pricing, service level agreements, location, integrity, access, segregation, breaches, and confidentiality are just a few of the cloud computing issues that Nepal is clearly encountering. According to the research, the three main areas of cloud computing security are storage, virtualization, and networks. Users and suppliers of cloud services are primarily concerned in virtualization, which enables several users to use a single physical server. Various forms of technological virtualization can present difficulties. Attacks on virtual networks often occur during communications with distant virtual equipment. They are aiming for data security. As one of the world's emerging nations, Nepal has to start making use of its own servers and satellites for data centers and connectivity.

References

[1] A.Leinwand, (2009)."The Hidden Cost of the Cloud: Bandwidth Charges," http://gigaom.com/2009/07/17/thehidden-cost-of-the- cloud-bandwidthcharges

[2] Amazon Elastic ComputeCloud. http://aws.amazon.com/ec2/

[3] Baburajan, R. (2011). "The Rising Cloud Storage Market Opportunity Strengthens Vendors
[4] ."http://it.tmcnet.com.
[5] Bele, S. B (2018). A Comprehensive Study on Cloud Computing. International Journal of Information Research and Review. Vol. 05, Issue, 03, pp.5310-5313
[6] Cloud Computing: Clash of the clouds", 2009. The Economist. www.economist.com.
[7] Cloud Security Alliance (2010). Top Threats to Cloud Computing V1.0. Available: https://cloudsecurityalliance.org/research/top-threats
[8] Conti, Marco, (2011)."Research challenges towards the Future Internet," Computer Communications, 34(18), 2115– 2134
[9] For a detailed analysis of NRENs in Europe and their role, see the documents (in particular the TERENA compendium), http: / /www.terena.org/publications/
[10] Google App Engine. http://code.google.com/appengine. Retrieved: 9February 2019.
[11] Grumman, G. (2008). What cloud computing means". InfoWorld. Retrieved: 10 February 2019.
[12] Hashizume (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications.
[13] http://cloudsecurity.org/2008/10/14/biggest-cloud- challengesecurity, retrieved 29 Feb 2019.
[14] 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
[15] Koslovski G., Huu T. T., Montagnat J., & Primet P. V.-B, 2009. First International Conference, CloudComp 2009. Munich, Germany, October 19-21.
[16] 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.
[17] Li Henry (2009). Introduction to Windows Azure An Introduction to Cloud Computing Using Microsoft Windows Azur.
[18] 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