Concerns and Difficulties with Cloud Computing Security

Chetan N. Rathod [1], Bhumika K. Charnanand [2]
[1]Vivekanand College for BCA, Surat
[2]Smt. Z.S. Patel College, Surat

Abstract:

A promising technology to aid in the creation of expansive, flexible, on-demand computing infrastructures is cloud computing. The conceptual and physical foundation for computing of the future has been established by cloud computing. A new business trend based on cloud technology has emerged as a result of the evolution of cloud-based services and service providers. But companies are setting themselves up for failure if cutting-edge technology supporting cloud computing lacks security. The organization's practice of regularly implementing this technology automatically added new risk on top of the already-existing risk. It goes without saying that putting everything into the cloud, or into a single box, will make things easier for hackers. In order to prevent issues like data loss or theft, cloud service providers and their clients should ensure that the cloud is sufficiently secure against external threats. This essay examines cloud computing from an overview perspective, highlighting various security risks and difficult problems.

Keywords:

Cloud Computing, SaaS, PaaS, IaaS, Virtualization, Security Issues, Threats

INTRODUCTION:

The scientific and industrial communities are beginning to recognise the growing significance of cloud computing. The primary goal of cloud computing, which is both a distribution architecture and a computational paradigm, is to offer fast, safe, and easy data storage and net computing services. All computer resources are visualised as services and supplied via the Internet. A variety of computing concepts and technologies, including Service Oriented Architecture, Viruses infect systems by acting like parasites. These programmes come in the form of files with the extension.exe or.com that manage other programmes. Upon clicking the.exe file on the computer, a virus may infiltrate the system, causing it to malfunction and necessitate a fresh format. In order to meet users' computing needs, Web 2.0, virtualization, and other Internet-based technologies offer common business applications online via web browsers, with users' software and data being stored on servers. [1] Adoption of cloud computing has numerous advantages, but there are also some major drawbacks. All of the data in a cloud computing environment is stored across a network of resources, making it possible to access the data using virtual machines. There are many different security and privacy issues that need to be recognised and addressed because these data centres could be located anywhere in the world, outside of users' reach and control. In order to identify the major threats found in the literature pertaining to cloud computing and its environment, this paper presents a categorization of security issues for cloud computing with a focus on the so-called SPI model (SaaS, PaaS, and IaaS).

CLOUD COMPUTING

Cloud computing, according to the National Institute of Standards and Technology, is a model that allows for easy, on-demand network access to a shared pool of reconfigurable computing resources, such as servers, networks, storage, apps, and services, that can be quickly provisioned and released with little involvement from service providers or management. Cloud computing is the cost-effective, location-independent sharing of resources on a larger scale. Cloud resources, such as those offered by Amazon, Google, IBM, and others, can be used by the client and deployed by the vendor. [2] Resources in a cloud-based computing infrastructure are typically located on someone else's site or network, and cloud users access them remotely. Processing is done remotely, which implies that information from an individual must be sent to a server or cloud infrastructure for processing, and that the output is returned once the necessary processing has been completed.

It may occasionally be necessary, or at the very least, feasible, for the individual to store data on distant cloud servers. These provide the following three delicate states that, in the operational context of cloud computing, are especially concerning:

- Sensitive personal data being sent to a cloud server
- Data transfer from the cloud server to the computers of clients and
- The remote, non-client-owned cloud servers used to store the personal data of customers.

Because the aforementioned three cloud computing states are all extremely vulnerable to security breaches, it is crucial to conduct research and analysis on the security aspects of cloud computing practices. [3]

RELATED WORKS

Goals for Cloud Information Security

According to the Data and Analysis Centre for Software (DACS), software cannot be deemed secure unless it possesses the following three attributes:

- Programmes that run reliably and accurately in a range of scenarios, such as when they are attacked or executed on a malicious host.
- Software with a low count of vulnerabilities or none at all that could jeopardise the reliability of the programme.
- Software with the capacity to recover from attacks as fast as possible while causing the least amount of damage possible.

Cloud Computing Security Concerns:

1. Software-as-a-service security issues:

SaaS offers on-demand application services, including CRM, ERP, email, and conference software. Out of the three core cloud delivery models, SaaS users have the least control over security. The following security issues could arise from the use of SaaS applications:

Application of Security: Usually, a Web browser is used to deliver these apps over the Internet. On the other hand, SaaS applications could become vulnerable due to web application flaws. Attackers have been breaking into user computers through the web and carrying out malicious tasks like stealing confidential information.

Security of Data: Any technology user is concerned about data security, but when SaaS users are dependent on their providers for adequate security, the issue becomes more significant. Organisational data processed in plaintext and stored in the cloud is common in SaaS. The security of the data while it is being processed and stored is the SaaS provider's responsibility.

Accessibility: Using a web browser to access internet applications simplifies access from any network device, including mobile and public computers. It does, however, also expose the service to more security vulnerabilities.

2. Platform-as-a-service security issues:

PaaS simplifies the deployment of cloud-based applications by doing away with the need to buy and manage the underlying hardware and software layers. Like SaaS and IaaS, PaaS depends on a secure web browser and a reliable, safe network. [4] PaaS application security consists of two software layers: the PaaS platform's runtime engine security and the customer apps that are installed on the platform. The data security problems that PaaS introduces are as follows:

Third party Relationships: In addition to standard programming languages, PaaS provides components of third-party web services, like mashups. Mashups blend several source elements together to create a cohesive whole. Therefore, data and network security concerns associated with mashups are also inherent to PaaS models.

Development Lifecycle: From the standpoint of application development, creating safe apps that could run on the cloud is challenging for developers. The System Development Life Cycle (SDLC) and security will be impacted by how quickly cloud applications evolve.

3. Issues with infrastructure-as-a-service security:

An online resource pool in the form of virtualized systems is made available by Infrastructure as a Service (IaaS). Users have the right to operate any software on the resources that have been assigned to them with complete control and management. These are a few of the IaaS-related security concerns:

Virtualisation: Users may run a range of applications by using virtualization to create, copy, share, migrate, and roll back virtual machines. However, because there is an additional layer that needs to be secured, it also presents new opportunities for attackers.
Virtual Machine Monitor: Since virtual machine isolation is the responsibility of the virtual machine monitor, or hypervisor, any compromise of the VMM could potentially affect its virtual machines as well. Like any traditional software, the VMM has security flaws because it is low-level software that manages and watches over its virtual machines.

Shared Recourses: On the same server, virtual machines can share resources like memory, CPU, and I/O. The security of each virtual machine (VM) may be compromised by resource sharing. For instance, without having to compromise the hypervisor, a malicious virtual machine (VM) can deduce certain information about other VMs through shared memory or other shared resources.

DIFFICULTIES IN CLOUD COMPUTING SECURITY

A newer technology that uses shared resources and is less expensive, cloud computing charges users on a pay-per-use basis based on usage. Owing to its characteristics, it may encounter numerous security threats and difficulties. These topics are covered and clarified in this section:

Data Loss: There is always a chance that data will be lost or stolen, whether it be through unintentional deletion, loss of the encryption key, or unauthorised access. For businesses, this is one of their biggest worries because, in addition to the risk of damage to their brand, they are legally required to protect it. [4]

Multi location of private data: If an organisation keeps its confidential information on a third party's device, that could be pretty risky. In a way, the confidential information of the companies is on another person's computer. Knowing which nation a company's data will be hosted in is crucial information.

Reused IP Addresses: When a specific user leaves a network, the IP address that was previously assigned to him is given to a new user. Even though a new user is occasionally given the old IP address, there is always a chance that another user will still be able to access the data because the address is still stored in the DNS cache and the data belonging to a specific user may be accessed by another user, infringing on their privacy. [5]

Denial-of-Service Attacks: A denial-of-service (DoS) attack aims to render the services allocated to authorised users inaccessible. The authorised user cannot access the service as a result of the attack because the server handling it is overloaded with requests. [6]

SOLUTIONS FOR CLOUD COMPUTING SECURITY CONCERNS

Investigation Support: Users are given access to audit tools to check policy enforcement and learn how their data is used, stored, and safeguarded. However, the investigation of illicit activity is highly challenging due to the possibility of data for multiple customers being geographically dispersed across a set of hosts and datacentres, as well as collocated. In order to resolve this audit, the evidence and the tools need to be contractually committed. [7]

Network Security: By employing IP Spoofing, a user can prevent access to any Internet-based service, potentially compromising security. We can use the digital signature technique to solve this. The Secure Socket Layer (SSL) Protocol is used to control message security over the Internet and prevent resource hacking.

Cryptography Algorithm: It goes without saying that cloud service providers use powerful encryption algorithms to protect user data. However, the issue with encryption is that it can accidentally render data completely unusable and complicate its availability. [8] In order to resolve this issue, the cloud provider needs to show proof that skilled professionals created and evaluated the encryption scheme.

Backup: Natural disasters may harm the actual devices, which could lead to data loss. Information backup is essential to the vendor's assurance of service in order to prevent this issue. V SOLUTIONS FOR CLOUD COMPUTING SECURITY ISSUE

CONCLUSION:

These days, cloud computing is all the rage, with many seeing it as the IT enterprise's next generation architecture. Despite having completely changed the computing industry, it is vulnerable to a wide range of security risks, from application-level to network-level. Controlling these security threats is necessary to maintain the Cloud's security. To protect the cloud against outside threats, regular auditing of the cloud is required. This paper presents a number of security concerns for cloud computing environments from a variety of angles, along with preventative measures. Concrete security standards for cloud computing may be created in the future. Advanced encryption techniques can be used for both cloud storage and data retrieval to ensure secure cloud data access. In order to distribute keys to cloud users in a way that restricts access to authorised individuals only, appropriate key management techniques should be employed.

REFERENCE:

[1] Mahbub Ahmed, “Above the Trust and Security in Cloud Computing: A Notion towards Innovation” - IEEE International Conference on Embedded and Ubiquitous Computing, 2013.

[2] Michael glas and paul Andres, “An Oracle white paper in enterprise architectureachieving the cloud computing vision”, CA-U.S.A, Oct 2010.

[3] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, Security Issues for Cloud Computing, International Journal of Information Security and Privacy, 4(2), 39-51, University of Texas, USA, April-June 2010.

[4] Joachim Schaper, 2010, “Cloud Services”, 4th IEEE International Conference on DEST,Germany.

[5] Dr. Gurdev Singh, Shanu Sood, Amit Sharma, “CM- Measurement Facets for Cloud Performance”, IJCA, , Lecturer, Computer science & Engineering, Eternal University, Baru Sahib (India), Volume 23 No.3, June 2011.

[6] R. Gellman, “Privacy in the clouds: Risks to privacy and confidentiality from cloud computing,” The World Privacy Forum, 2009. http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

[7] Dukaric, R. and Juric, M.B. (2013). Towards a unified taxonomy and architecture of cloud frameworks. Future Generation Computer Systems, 29, 1196–1210. doi:10.1016/j.future.2012.09.006

[8] Emam, A.H.M. (2013). Additional Authentication and Authorization using Registered Email-ID for Cloud Computing. International Journal of Soft Computing and Engineering, 3(2), 110-113.