Medicon Engineering Themes
Volume 1 Issue 3 December 2021
Editorial Note

Cloud Computing Security Issues

Muhammad Imran Tariq*

Department of Computer Science, Superior University, Lahore, Pakistan

***Corresponding Author:** Muhammad Imran Tariq, Department of Computer Science, Superior University, Lahore, Pakistan.

Received: October 16, 2021; **Published:** December 03, 2021

Handheld devices captured the world and now every person who is technology dependent is replying upon the cloud computing. The rapid growth in the user of the mobile computing arises various question and opened new dimensions of research. Now, the universities and industry stake holders are looking new ideas to maximum utilize the mobile computing benefits and give maximum relief to its customers. This mobile computing and cloud computing gives both hardware and software advantages and also new concepts.

Cloud computing being the new technology in the field of information technology is the most recogonized and emerging technology. In past, lot of researches have been conducted to find the different areas of cloud computing but still few areas are still needs to be explored including the security, privacy, business values. The most hot topics that needs to be explored are current gaps and trends. The industry reports and practical experiences should be given most weightage. We needs to highpoint the importance of the cloud computing and its security and privacy issues.

Cloud computing is facing lot of serious nature of technical challenges since last two decades. In last year's, computing has become very cheap, easily accessible, and in reasonable amount for various business and individual. These advantages attracted many companies, especially small and medium enterprises to adopt the cloud software and hardware services with very little cost. The cloud customers can achieve their business robustness and get great profit from the cloud environment.

The core roadblock in the adoption of the cloud computing is the cloud service provider and many organizations are not agreed with the terms and conditions of the cloud service providers due to their security and privacy challenges. Trust is the main thing that cloud service provider needs to win and make sure their customers that their organizations can mitigate all types of the risks, attacks, vulnerabilities, virtualization issues, and cloud vender is complied with information security standards. Here we discussed the three most considered security factors for the cloud system that are confidentiality, integrity and availability (CIA). Although, the CIAdomain is a widely used convention for determining the security problems of a traditional information system but we discussed it with the context of cloud computing.

Data Confidentiality includes data segregation, geographical location, incomplete deletion of the data by the vender, data backup services are untrusted, inadequate monitoring of data logs, access to encryption schemes, and cloud user access to privileged data. Virtualization confidentiality includes root privileges, Virtual Machine migration, workload isolation, virtual machine images, and virtual local area network.

Data Integrity includes data outsourcing, SQL injection, cross scripting attacks, metadata spoofing attack, wrapping attacks, virtual machine instance, virtual machine replication, virtual machine rollback, virtual machine live migration, virtual machine escape and hopping, and lifecycle of virtual machine.

Data Availability includes Denial of Service attack, indirect Denial of Service, customer penetration testing, third party destruction, natural disasters, and virtualization availability.

Volume 1 Issue 3 December 2021