Cloud computing is a framework for providing various computing and storage services on the on-demand basis via the internet. It provides access to a user pool of shared network and storage resources using the server of the service provider without materially acquiring these resources. Hence, it saves managing cost and time for various organizations as well as individual users. Many industries, such as education, banking, healthcare and manufacturing are widely adapting cloud services due to their efficiency, flexibility and reduction of costs. Since, cloud services are universally accessible; it makes accessing data process a lot easier than traditional storage methods. Some popular cloud providers where client data is stored and maintained are Google, Amazon, SalesForce, Microsoft, etc. However, cloud technology is completely internet dependent and hence, faces as many threats as that are existing in the networks such as intranets. These threats can occur in various forms such as traffic hijacking, insecure interface and APIs, malicious insiders, abuse of cloud services, shared technology vulnerabilities, data breaches, perimeter security model broken or unknown risk profile. The primary objective of this paper is to acknowledge the major issues of security and provide a
solution to overcome them.

References

16. A. Ashok Kumar, Santhosha and A. Jagan, “Two layer Security for data storage in cloud,”
Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), 2015 International Conference, February 2015.

Index Terms

Computer Science  Security

Keywords

Cloud Computing, Data Security, Compression, Encryption, Authenticity, Integrity