Abstract

Cloud Computing can be defined as a technology that allows access to computing resources and services in a flexible, scalable and highly available manner over the internet. It has been gaining momentum over the years with several organizations targeting cloud migration from the conventional on-premise approach for their data centers. Cloud Service Model offerings such as Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS) has grown in adoption with cloud data storage being one of the popularly used services in the public cloud. With the widespread growth of cloud computing services, new security and privacy issues have arisen, posing an open challenge to adoption of the cloud computing paradigm. Authentication stands to play an important role in mitigating the security and privacy issues foreseen. There is a need to enhance the current authentication schemes in use which are known to be prone to security threats and attacks. Multi-factor authentication allows the use of more than one authentication factor; knowledge, possession and inherence with combinations of the first two currently being used by most cloud service providers however still facing security breaches. In this paper, the author discusses security threats in cloud
computing, the current multifactor authentication mechanisms in use and how to enhance multifactor authentication using fingerprint biometrics in cloud computing data storage to assure confidentiality and integrity of user data.

References

Index Terms

Computer Science  Security

Keywords

Biometric, Multifactor Authentication, Fingerprint Scanning, Cloud Computing