Abstract

Cloud database services assure the high availability and scalability, but there are many issues about data privacy and confidentiality. The online applications are also vulnerable to attack that gain access to the sensitive data as the attacker can easily exploit software bug. Hence the security and privacy of the sensitive data stored on the cloud is the biggest challenge today. Storing critical and sensitive data in the hands of cloud service provider will not guarantee the privacy of data. Several ways are available for storage services, but the data privacy and confidentiality solutions for cloud database are still in research. The data privacy and confidentiality can be maintained by combining encryption of data with SQL operations. The application that uses SQL database can be secured by using DD-PLAC architecture which provides confidentiality of the data stored on cloud. DD-PLAC (Distributed Database with Proxy-less architectures that store meta data in the cloud) architecture combines data encryption, key management and access control policies which addresses the issues related to typical threat for cloud database.
References

9. Tim Mather, Subra Kumaraswamy, and Shahed Latif "Cloud Security and Privacy" Published by O'Reilly Media, Inc.
10. Carlo Curion, Evan P.C.Jones, Hari Balkrishna, Nirmesh Malviya, "Relational Cloud: A Database as a Service for the Cloud"
Index Terms

Computer Science  Security

Keywords

Security, Privacy, cloud database, Symmetric key algorithm (SKA), access control, DD-PLAC (Distributed Database with Proxy-less architectures that store meta data in the cloud)