Enhancing Security in Public Clouds using Data Anonymization Techniques

Abstract

Security issues have given rise to immersing an active area of research due to the many security threats that most of the organizations have faced at present. Despite the advancements in cloud computing, the organizations are slow in accepting it, due to security threats that make a cloud environment to be source of data breaching. Maintaining privacy for the high dimensional database has become an important aspect of security. This paper, emphasizes on protecting the data in public cloud using data anonymization techniques. Anonymization is the process of making the sensitive data to be de-identified and preventing this data to be linked with identities of an individual or an organization. The data has to be anonymised, thereby preventing it from malicious attack & at the same time data must be also made available for the owner of the data. To preserve the data from the attacker, two methods of privacy preserving models are used - k-anonymity and l-diversity. Finally, in this paper an algorithm for graph anonymisation is presented, called the Evolutionary Algorithm for Graph Anonymization (EAGA) that is based on k-anonymity model.
References

1. k-Anonymity” – P.Samarati, S.Foresti, S. De Capitani, Università degli Studi Milano, Italia.

Index Terms

Computer Science

Distributed Systems

Keywords

Data anonymization, Cloud Computing, k-anonymity, l-diversity