Abstract

More than one data provider collaborate to publish their data is considered here. m-privacy is a technique proposed to defend m-adversary during collaborative data publishing. M-privacy satisfies the privacy problem while publishing sensitive data. Apart from providing privacy to published data, it is also necessary to provide security between the data provider and third party/un-trusted server, to ensure this, Secure multiparty communication (SMC) protocol is used to provide secure data transfer from publisher and server. There were techniques such as k-anonymity, l-diversity, t-closeness, which were proposed to handle external attacks in data publishing, but none is published for considering internal attacks. This m-privacy is a technique, which considers internal attacks.

AIM: The goal is to publish an anonymized view of the integrated data such that a data recipient including the data providers will not be able to compromise the privacy of the individual records provided by other parties.
M-Privacy for Collaborative Data Publishing

References


Index Terms

Computer Science Information Sciences

Keywords

Annoymization, Adversary, TTP, SMC.