Insider Collusion Attack on Privacy-Preserving Kernel-Based Data Mining Systems

In this paper, we consider a new insider threat for the privacy preserving work of distributed kernel-based data mining (DKBDM), such as distributed support vector machine. Among several known data breaching problems, those associated with insider attacks have been rising significantly, making this one of the fastest growing types of security breaches. Once considered a negligible concern, insider attacks have risen to be one of the top three central data violations. Insider-related research involving the distribution of kernel-based data mining is limited, resulting in substantial vulnerabilities in designing protection against collaborative organizations. Prior works often fall short by addressing a multi factorial model that is more limited in scope and implementation than addressing insiders within an organization colluding with outsiders. A faulty system allows collusion to go unnoticed when an insider shares data with an outsider, who can then recover the original data from message transmissions (intermediary kernel values) among organizations. This attack requires only accessibility to a few data entries within the organizations rather than requiring the encrypted administrative privileges typically found in the distribution of data mining scenarios. To the best of our knowledge, we are the first to explore this new insider threat in DKBDM. We also analytically demonstrate the minimum amount of insider data necessary to launch the insider attack. Finally, we follow up by introducing several proposed privacy-preserving schemes to counter the described attack.