In this position paper, we present a novel approach tosecuring personal and business data in the Cloud. We proposemonitoring data access patterns by profiling user behavior

to determine if and when a malicious insider illegitimatelyaccesses someone’s documents in a Cloud service. Decoydocuments stored in the Cloud alongside the user’s realunauthorized data access or exposure is suspected, and laterverified, with challenge questions for instance, we inundate themalicious insider with bogus information in order to dilutethe user’s real data. Such preventive attacks that rely ondisinformation technology, could provide unprecedented levelsof security in the Cloud and in social networks. The results of our experiments suggest that user profilesare accurate enough to detect unauthorized Cloud access [9].When such unauthorized access is detected, one can respond

by presenting the user with a challenge question or with adecoy document to validate whether the access was indeedunauthorized, similar to how we used decoys in a local filesetting, to validate the alerts issued by the anomaly detectorthat monitors user file search and access behavior. The advantages of placing decoys in a file system are threefold:(1) the detection of masquerade activity (2) the confusion

of the attacker and the additional costs incurred to distinguishreal from bogus information, and (3) the deterrence effectwhich, although hard to measure, plays a significant role inpreventing masquerade activity by risk-averse attackers.