**Summary of “Fraud De-Anonymization For Fun and Profit”**

**Name:** Avineet Kumar Singh

**ID#:** M12135865

**Abstract.** Popular online service providers rely on user feedback to rank products and content they host over the Internet. This leads to search rank fraud in online, peer-opinion systems, made possible by crowd sourcing sites and specialized fraud workers. For this reason, most major online, peer-opinion services seek to detect and remove fake reviews that result from hidden endorsements. In this paper, theauthors have studied the search rank fraud de-anonymization problem and shown that it is different from the well-studied fraud or spammer detection problem. They introduced a fraud de-anonymization approach to disincentivize search rank fraud. UODA, an unconstrained optimization de-anonymization approach that attributes a fraudulent user account to the fraud worker with the highest likelihood of having generated its review history was introduced. DeepCluster was developed, a semi-supervised approach to cluster user accounts based on deep learning features extracted from the common activities of the accounts. DeepCluster was leveraged to build a co-ownership predictor which was further used to introduce DDA, a discriminative de-anonymization solution, and PFD, a pseudonymous fraudster discovery algorithm that clusters fraudulent accounts that cannot be attributed to known workers. Authors introduced a Detego, a system that combines fraud de-anonymization with fraudster discovery to iteratively expand both knowledge of identifiable fraud workers and the accounts that they control. The first cheating-resistant fraud de-anonymization validation protocol was introduced, that transforms human fraud workers into ground truth, performance evaluation oracles. In a user study with 16 human fraud workers, UODA achieved a precision of 91% and co-ownership predictor significantly outperformed a state-of-the art competitor, and tens of new fraud workers were discovered.

**Contributions.** Through this paper authors introduced the first cheating-resistant, fraud de-anonymization validation protocol, to obtain ground truth confirmation on the performance of developed solutions as compared to old fraud detection solutions whose accuracy was difficult to evaluate.

The authors also developed a graph based deeplearning approach to predict ownership of account pairs by the same fraudster which helped to discover tens of new fraud workers, and attribute thousands of suspicious user accounts to existing and newly discovered fraudsters.

**Weaknesses.** The author has assumed that the 16 participants were honest, which may not be correct. There is a possibility that the participants didn’t provide correct data and Detego can effectively provide fraud de-anonymization only in the presence of seed ground truth information about accounts controlled by known fraudsters.