Casey Astiz
Adviser: Professor Linderman
September 17, 2018

Combating Fraud By Leveraging Machine Learning and Human Behavior

The main goal of this thesis is to investigate current methods of fraud detection and implement one or more of those methods in financial contexts. I plan to to research what the most prevalent methods for fraud detection are currently, as well as look at what was being done in the past. Fraud detection is a difficult field of study because it falls in the subset of anomaly detection and has very skewed classes as more transactions are not fraud than are fraud, and the classification of fraud is always changing. In order to build an effective fraud detector, it must be adaptive to new patterns and categories of fraud that are developing as fraudsters find new methods to deceive the system.

The main feature of this thesis will be a review of different methods used in the industry in the past and today for fraud detection, as well as my own implementation using some dataset of transactions to be determined. I plan to search Kaggle and other databases for a potential real world source of transactions, and possibly explore a dataset from the Financial Services Technology Consortium [1]. This background section will include information from published research papers as well as information I learn from interviewing people at different companies in this field to provide some context for the literature review. Through my internship, I had the opportunity to interview someone on the Apple Pay fraud team, and was able to ask about techniques, methods and difficulties faced in the Apple Pay context. Comparing business interactions with fraud to published research in the field will allow me to somewhat analyze the performance of different machine learning methods in real life versus a research context.

The implementation portion of this thesis will be based on the review of current methods and will use a large dataset of financial transactions including fraudulent transactions. The goal is to use a large dataset of real transactions, potentially from a bank or other financial institution, with any references to the real users obscured. However, this may not be available information in which case I will use either a combination and real and synthetic transaction data or a fully synthetic dataset. I plan to implement one of the architectures I have read about, such as in "Combining Data Mining and Machine Learning for Effective User Profiling" [2]. I will then conduct experiments where I will test different machine learning models like support vector machines, neural networks, CART, C4.5, RIPPER, and BAYES to look for highest performance [3][4]. I will also vary number of total transactions and proportion of fraud to legitimate transactions throughout these experiments.

In addition to the above, I would also like to discuss both privacy and game theory in relation to fraud. Privacy is a big concern when trying to detect fraud. If a company were to have someone's location as well as their SSN, transaction history and other information, then fraud detection is a relatively straight forward. In an Apple Pay and other internet payment contexts, a user does not go through Customer Identification Program (CIP) until they have spent 500 dollars on their account. Before this point, there is no verification that the credit card user matches the credit card owner, and leads to a large quantity of smaller fraud transactions. Past this point, CIP has been performed, and fraud is much easier to detect. For companies who are concerned with the privacy of their users and that do not want to force users into CIP when signing up for a service, fraud detection has the added limitation of having to work with limited information. I think there is a lot more to privacy protection that I do not know or understand, and I would like to research the challenges and solutions to these problems that have been discovered so far.

Game theory is also an important element of fraud detection. Unlike other forms of anomaly detection, these are real people who are creating these new patterns. As new restrictions are enforced, fraudsters will find new and crafty ways to get around them. Part of fraud detection and prevention is to make educated guesses about how a user or a group of users behave given new restrictions. I think there is a lot to be learned about human interactions with human designed systems, especially in this complicated context [5].

A possible extension is to investigate other applications for these adaptive skewed class models. For example, these methods could be applicable in bioinformatics, biometric fraud, or in other non-financial fraud contexts. If there is available time and I can obtain a relevant dataset, I propose to evaluate my fraud detector in one of these other contexts.

References:

[1] Stolfo, Salvatore J., Fan, David W., Lee, Wenke, and Prodromidis, Adreas L. “Credit Card Fraud Detection Using Meta-Learning: Issues and Initial Results.” AAAI Press, 1997. Pages 83-90. http://www.aaai.org/Papers/Workshops/1997/WS-97-07/WS97-07-015.pdf

[2] Fawcett, Tom and Provost, Foster. “Combining Data Mining and Machine Learning for Effective user Profiling.” AAAI Press, 1996. Pages 8-13. http://www.aaai.org/Papers/KDD/1996/KDD96-002.pdf

[3] Chan, Philip K. and Stolfo, Salvatore J. “Toward Scalable Learning with Non-uniform Class and Cost Distributions: A Case Study in Credit Card Fraud Detection.” KDD'98 Proceedings of the Fourth International Conference on Knowledge Discovery and Data Mining. Pages 165-168. http://www.aaai.org/Papers/KDD/1998/KDD98-026.pdf

[4] Perols, Johan. “Financial Statement Fraud Detection: An Analysis of Statistical and Machine Learning Algorithms.” A Journal of Practice & Theory: May 2011, Vol. 30, No. 2. Pages 19-50. http://aaajournals.org/doi/10.2308/ajpt-50009?code=aaan-site

[5] Vatsa V., Sural S., Majumdar A.K. “A Game-Theoretic Approach to Credit Card Fraud Detection.” In: Jajodia S., Mazumdar C. (eds) Information Systems Security. ICISS 2005. Lecture Notes in Computer Science, vol 3803. Springer, Berlin, Heidelberg. https://link.springer.com/chapter/10.1007/11593980_20

[6] Bose, Indranil and Mahapatra, Radha K. “Business data mining- a machine learning perspective.” *Information & Management*, Volume 39, Issue 3, 20 December 2001, pages 211-225. https://www.sciencedirect.com/science/article/pii/S037872060100091X