CLOUD FILE SHARING AND DATA SECURITY THREATS – EXPLORING THE EMPLOYABILITY OF GRAPH-BASED UNSUPERVISED LEARNING IN DETECTING AND SAFEGUARDING CLOUD FILES

Harshit Yadav

Student, Bal Bharati Public School, Dwarka, New Delhi

ABSTRACT

As increasingly more enterprises are deploying cloud file-sharing services, this adds a new channel for potential insider threats to company data and IPs. In this paper, we introduce a two-stage machine learning system to detect anomalies. In the prelim stage, we anticipate the entrance logs of cloud record sharing administrations onto relationship diagrams and use three complementary graph-based unsupervised learning methods: OddBall, PageRank and Local Outlier Factor (LOF) to generate outlier indicators. In the second stage, we outfit the exception pointers and present the discrete wavelet change (DWT) strategy, and propose a method to utilize wavelet coefficients with the Haar wavelet capacity to distinguish anomalies for insider danger. The proposed system has been deployed in a real business environment, and demonstrated effectiveness by selected case studies.

Keywords*—discrete wavelet transform; Haar wavelet; insider threat detection; cloud file-sharing; graph-based unsupervised learning*

INTRODUCTION

Enterprise file sharing, whether on the cloud (public, hybrid, or private) or on-premises, enables individuals to share files from mobile devices and PCs. Sharing can happen between people (for example, partners and customers) within or outside the organization, as well as between applications. The offerings enable modern user productivity and collaboration scenarios for the creation of a digital workplace [Basso et al., 2016]. However, cloud file-sharing creates a new channel for insider threats, including the leakage and exfiltration of business strategies, customer information, personal identifiable information (PII), company IPs, source code, etc.

Depending on the vendors that provide enterprise file sharing services, certain levels of security and data protection in cloud services are offered. These include password protection, data encryption, data loss prevention, disaster recovery management, and security analytics.

However, most of these are rule-based, and generate a lot of alerts with a high false positive rate. In addition, many of the alerts are related or duplicated, which overwhelms the capacity of the security operations center (SOC) to investigate all of them. In this examination, we build up a two-arrange machine learning framework to naturally recognize client abnormal conduct dependent on the entrance logs of cloud document sharing frameworks and feed a little specific gathering of clients to the SOC for examination. The architecture of our proposed machine learning system is shown in Fig. 1.

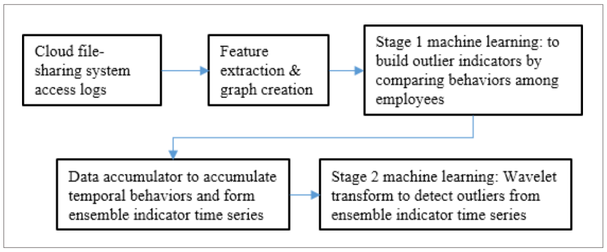

Cloud file-sharing system access logs
Feature extraction & graph creation
Stage 1 machine learning: to build outlier indicators by comparing behaviors among employees
Data accumulator to accumulate temporal behaviors and form ensemble indicator time series
Stage 2 machine learning: Wavelet transform to detect outliers from ensemble indicator time series

Fig. 1. Architecture of machine learning system for cloud file-sharing outlier detection

Specifically, we use graph-based OddBall [Akoglu et al., 2010, Akoglu et al., 2015] and PageRank [Page et al., 1999] algorithms, as well as the density-based Local Outlier Factor (LOF) algorithm [Breunig et al., 2000]. Each algorithm will generate an outlier indicator for every user based on their behavior relative to the others on a daily basis. The reason we use three different algorithms is that they may capture different characteristics as shown in Section 5.

Then we accumulate the daily outlier indicators to create time series for each user and use it to detect outliers from a temporal perspective. To use the benefits of multiple complementary indicators, and avoid the weaknesses of using a single indicator, we follow the suggestions of [Zimek et al., 2014], and adopt the average function to form an ensemble of outlier indicators from Oddball, PageRank, and LOF.

In order to identify suspicious insiders from the ensemble score time series, we propose to use the wavelet transform method, which is inspired by [Bilen and Huzurbazar, 2002; Grané and Veiga, 2010]. To the best of our insight, we have not seen research applying this method to the abnormal file sharing problem in the cyber security insider threat detection domain. In summary, our main contributions are:

- We create a machine learning system to detect behavioral outliers in cloud file-sharing for the purpose of malicious insider detection.

- We project the audit trail data into relationship graphs and apply three complementary unsupervised learning algorithms to generate outlier indicators by comparing different users' behaviors at a particular point of time.

- We introduce a wavelet transform approach to take into account users' temporal behavior as well as the severe scale, and to form a single wavelet-based risk score.

The rest of the paper is sorted out as pursues. Section

II briefly describes DWT and the Haar wavelet funcion, which is the core method in our study. Section III shows experimental results. Section IV concludes the whole paper.

WAVELET TRANSFORM

A. Discrete Wavelet Transform

A wavelet transform maps a one-dimensional function into a two-dimensional function (e.g. "time" and "scale"). Formally, in a wavelet transform analysis application, the first step is to adopt a wavelet function, or mother wavelet. At that point, fleeting examination is performed with a contracted, high-recurrence variant of the mother wavelet, while recurrence investigation is performed with an enlarged, low-recurrence adaptation of a similar wavelet. Because the original function can be represented in terms of a wavelet expansion, data operations can be performed using just the corresponding wavelet coefficients.

DWT refers to wavelet transforms for which the wavelets are discretely sampled, and in our study, we focus on the DWT. The generic form of a one-dimensional DWT is shown in Fig. 2 (from goo.gl/Wm1EQz). Here an original function X(n) is passed through a high and low frequency filters, *h* and g, respectively. Both *h* and g are self-orthogonal and are orthogonal to one another. Then we apply DWT by a down- sample factor of 2, and we get the level 1 coefficients d11(n) from high frequency filter, and d10(n) from low frequency filter g. Multiple levels of the wavelet transform are made by repeating the filtering and decimation process on the low filter outputs only (i.e. di0(n)). The process is typically carried out for a finite number of levels K. The resulting coefficients di1(n), i∈ {1··· K} and dK0(n) are called wavelet coefficients.

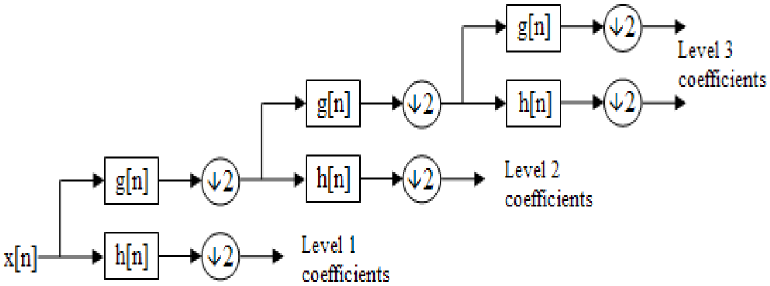


Fig. 2. Discrete wavelet transform

In our problem, each user has multiple time series from different outlier indicators (i.e., OddBall, PageRank and LOF), and we generate an ensemble of outlier indicators with the average function. Then based on the one-dimensional ensemble time series we apply DWT to detect outliers.

B. The Haar Wavelet Function

Wavelets are defined by the wavelet function $f(t)$ (i.e. the mother wavelet) and scaling function φ(t) (also called the father wavelet). The $f(t)$ is a function used to divide a given function into different scale components, with some particular properties, such as: wave-like oscillation, integral value is zero, and the integral value of its square format is unity.

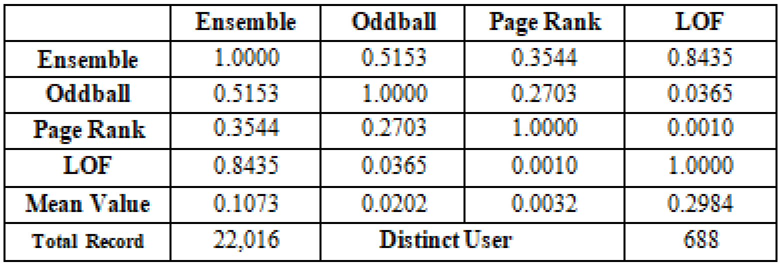
EXPERIMENT RESULTS AND DISCUSSIONS

In our experiment, we use 3 months of Symantec Box cloud file-sharing access log data. The input dataset has 22,016 observations from 688 unique users. In this section, we will elaborate our results and provide discussions.

A. Correlations between Outlier Indicators and ensemble

Ideally all three outlier indicators (i.e. OddBall, LOF, and PageRank) would be positively correlated, giving us more confidence in them. Table I shows the correlation matrix. For OddBall and PageRank, the correlation coefficient value is about 0.2703. The other two pairs are smaller, but still positive. The weak correlations between OddBall and LOF scores implies that combining these outlier indicators may yield better detection performance. Therefore, we take the arithmetic ensemble of arithmetic averaging Oddball, LOF, and PageRank outlier indicators and create a new time series. This new time series generates stronger correlation with each of the individual outlier indicators. The DWT will be applied to the new time series to generate the final outlier score.

TABLE I. CORRELATION MATRIX



	Ensemble	Oddball	Page Rank	LOF
Ensemble	1.0000	0.5153	0.3544	0.8435
Oddball	0.5153	1.0000	0.2703	0.0365
Page Rank	0.3544	0.2703	1.0000	0.0010
LOF	0.8435	0.0365	0.0010	1.0000
Mean Value	0.1073	0.0202	0.0032	0.2984
Total Record	22,016	Distinct User		688

B. Time Series Patterns of Outlier Indicators and Wavelet Risk Score

In this section, we randomly sample two users and look into details of the trending relationship between the ensemble outlier indicator and the Wavelet risk score to make sure that wavelet risk score is able to detect changes in the ensemble outlier indicator time series and effectively flag potential insider threat.

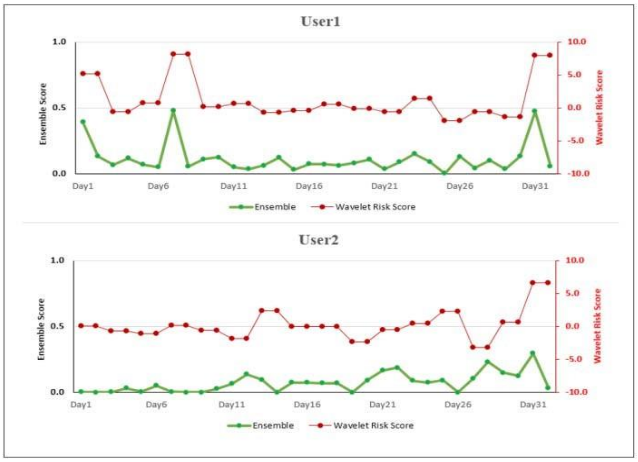


Fig. 3. Trend plots of Ensemble score and Wavelet risk score (over 32 days)

Fig. 3 shows the two users' daily ensemble values, and the Wavelet risk scores over a 32-day period. Note that Ensemble series use the vertical axis on the left, while the Wavelet risk score uses the vertical axis on the right. The figure shows that the Wavelet risk scores are closely correlated with Ensemble scores and the Wavelet risk scores show big spikes when the ensemble value increases significantly. However, the more important characteristic is that the wavelet risk score can detect subtle changes in the ensemble outlier indicator, for example for user 1, the ensemble outlier indicator looks like having a regular fluctuation during days 21-25 as in the other time intervals (the green line of the top chart in Fig 3), but there is a much clearer indication of the wavelet score (the red line of the top chart in

Fig 3). And later investigation proves that this is a significant detection. It is this that demonstrates the benefit of using DWT to generate wavelet risk score for potential insider threat detections. By adjusting the wavelet risk score threshold, we can send a very small number of alerts for SOC to investigate.

In summary, the Wavelet risk score from the first level coefficients of the Haar DWT is able to capture the patterns in both the outlier indicator feature space and temporal space and we propose to use that to flag risky users.

CONCLUSIONS AND DISCUSSIONS

In this paper, we propose a novel two-organize machine learning framework which use cloud record sharing access information to consequently recognize client atypical conduct for potential insider risk. In the first stage, we project the access log data onto user/file and user/user relationship graphs and apply three unsupervised algorithms to generate outlier indicators. In the second stage, we ensemble the outlier indicators and introduced the DWT with the Haar wavelet function to model users' temporal behavior for insider threat detection. Our experiment results demonstrate that the first level coefficients of the DWT with the Haar wavelet is able to effectively capture the temporal patterns of the user behaviors.

As for future work, we will incorporate more data sources, including but not limited to, active directory logs, windows logon logs, physical security logs, and printer logs, to better detect insider threats holistically.