Combating Insider Threat in the Open-World Environments: Identification, Monitoring, and Data Augmentation

Dawei Zhou

Department of Computer Science
Virginia Tech, VA, USA
zhoud@vt.edu

Abstract

Recent years have witnessed a dramatic increase in a class of security threats known as "insider threats". These threats occur when individuals with authorized access to an organization's network engage in harmful activities, potentially leading to the disclosure of vital information or adversely affecting the organization's systems (e.g., financial loss, system crashes, and national security challenges). Distinct from other types of terror attacks, combating insider threats exhibits several unique challenges, including (1) rarity, (2) non-separability, (3) label scarcity, (4) dynamics, and (5) heterogeneity, making themselves extremely difficult to identify and mitigate. We target the challenging problem of combating insider threats in open-world environments by leveraging a variety of data sources (e.g., internal system logs, employee networks, human trafficking, and smuggling networks). To effectively combat these intricate threats, we introduce an interactive learning mechanism that is composed of three mutually beneficial learning modules: insider identification, insider monitoring, and data augmentation. Each module plays a crucial role in enhancing our ability to detect and mitigate insider threats, thereby contributing to a more secure and resilient organizational environment.

Introduction

Our research goal is to build an interactive learning mechanism for insider threat detection on open-world data (Zhou and He 2023; Zhou 2021; Wu et al. 2023), which can be deployed to solve diverse tasks, ranging from insider characterization to insider tracking; from representing insiders in a salient embedding space to interpreting the prediction results; from mimicking the underlying distribution of insider threats to data augmentation. As shown in Figure 1, the proposed framework consists of three key modules: (M1) Insider Identification: characterize the descriptive and essential properties of insiders and detect groups of insiders with common traits (e.g., traitors, masqueraders, and unintentional perpetrators). (M2) Insider Monitoring: track the evolution of insider behaviors over time and provide a visual analytic system for analysis, annotation, and diagnosis. (M3) Data Augmentation: sanitize input data (e.g., completing missing data and cleaning noisy data) and generate

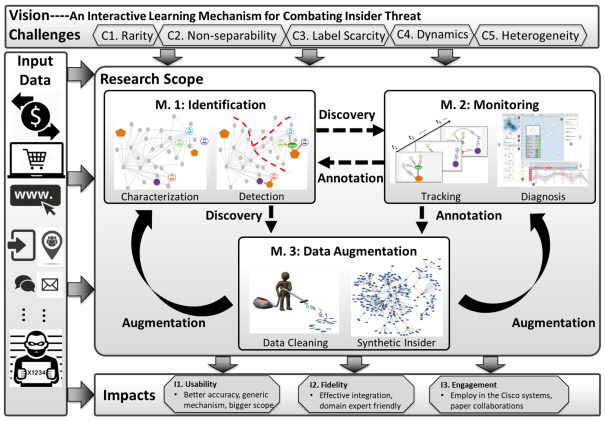

Figure 1: Research overview.

synthetic insiders to alleviate the label scarcity issue. The proposed mechanism operates through a *mutually beneficial synergy* among these three modules, where M1 serves as the *de-novo* step to characterize and identify potential insider threats without or with limited annotated data; M2 aims to provide a proper lens (e.g., from the right/relevant data sources, in the subspace spanned by the right/relevant attributes, at the right/relevant time steps) to examine and interpret the outputs from M1 and M3; M3 incorporates the discoveries from M1 and M2 to mimic the underlying data distribution and thus enable task-specific data augmentation.

Acknowledgements

This work is supported by Cisco, Deloitte, Commonwealth Cyber Initiative, 4-VA, and Virginia Tech. The views and conclusions are those of the authors and should not be interpreted as representing the official policies of the funding agencies or the government.

References

Wu, L.; Lei, B.; Xu, D.; and Zhou, D. 2023. Towards reliable rare category analysis on graphs via individual calibration. In *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, 2629–2638.

Zhou, D. 2021. *Harnessing rare category trinity for complex data*. Ph.D. thesis.

Zhou, D.; and He, J. 2023. Rare Category Analysis for Complex Data: A Review. *ACM Computing Surveys*, 56(5): 1–35.