RADemics

Advanced Persistent Threat Identification in Cloud Infrastructures Using Tensor-Based Machine Learning Approaches

S Sreejith Sreekandan Nair, Muralidharan J

LEADING FINANCIAL FIRM, KPR INSTITUTE OF ENGINEERING AND TECHNOLOGY

Advanced Persistent Threat Identification in Cloud Infrastructures Using Tensor-Based Machine Learning Approaches

[1]Sreejith Sreekandan Nair, Independent Research Scholar, Leading Financial Firm, Dallas, Texas, USA. hisreenair@gmail.com

[2]Muralidharan J, Associate Professor, Department of ECE, KPR Institute of Engineering and Technology, Coimbatore - 641407, Tamil Nadu, India. muralidharanae@gmail.com

Abstract

Advanced Persistent Threats (APTs) pose a significant challenge to cloud infrastructures due to their stealthy, multi-stage attack strategies. This chapter explores the role of tensor-based machine learning approaches in identifying APTs by leveraging the multi-dimensional nature of cloud security data. Traditional machine learning models often struggle to analyze large-scale, complex data generated in cloud environments. Tensor-based techniques, such as decomposition and factorization, provide effective methods for extracting hidden patterns, anomalies, and APT indicators across temporal, spatial, and user behavior dimensions. The chapter also addresses critical challenges, including latency, scalability, and real-time implementation of tensor models in dynamic cloud infrastructures. By comparing tensor-based methods with traditional approaches, the advantages in handling high-dimensional data are demonstrated. Finally, optimization strategies and distributed frameworks are discussed to enhance real-time APT detection. This work contributes to advancing cloud security systems through efficient, scalable, and robust tensor-based methodologies.

Keywords: APT detection, Tensor decomposition, Cloud security, Multi-Dimensional Data, Machine learning, Real-time anomaly detection.

Introduction

The rapid adoption of cloud infrastructures has revolutionized data storage, computation, and accessibility for businesses and individuals worldwide [1]. However, this widespread adoption has also amplified security concerns, particularly in the face of Advanced Persistent Threats (APTs) [2]. APTs are sophisticated, stealthy, and prolonged cyberattacks that target cloud systems to compromise sensitive data or disrupt services [3]. Unlike traditional cyber threats, APTs are multi-dimensional and evolve over time, making them exceptionally difficult to detect and mitigate [4]. Cloud environments generate massive volumes of multi-dimensional data, including network traffic, user behaviors, logs, and temporal patterns [5,6]. Therefore, effective APT detection requires advanced computational approaches capable of analyzing and extracting actionable insights from this complex data [7-9].

Traditional machine learning models have been widely applied to anomaly detection and threat identification [10]. However, these methods often face limitations when handling high-dimensional and dynamic cloud data [11]. Most conventional approaches rely on simplified, two-dimensional representations, which fail to capture the intricate relationships and latent patterns in multi-dimensional data [12]. The inability to model temporal, spatial, and user-behavioral correlations within cloud infrastructures diminishes their efficacy in identifying subtle APT indicators [13]. This necessitates innovative techniques that can effectively process and analyze multi-dimensional datasets to detect evolving threats with higher precision [14-16].

Tensor-based machine learning approaches have emerged as a promising solution to overcome these limitations [17]. Tensors, which are multi-dimensional generalizations of matrices, provide a robust framework for representing and processing cloud security data [18]. Techniques such as tensor decomposition and tensor factorization enable the extraction of hidden patterns and anomalies from high-dimensional datasets. These methods not only enhance feature extraction but also improve the accuracy and efficiency of APT detection in dynamic cloud environments [19-21]. By leveraging the strengths of tensors, it becomes possible to identify subtle threat indicators that would otherwise remain undetected by traditional approaches [22].

Real-time detection of APTs remains a significant challenge due to the massive scale and velocity of cloud-generated data [23]. Tensor-based models must address critical issues such as latency and scalability to be effective in real-world cloud infrastructures [24]. Optimizing tensor computations through hardware acceleration, approximate methods, and distributed frameworks can help overcome these challenges [25]. Such solutions ensure that APT detection systems can operate seamlessly in real-time, providing timely identification and mitigation of threats. This capability was critical for minimizing the impact of APTs on cloud services and ensuring the integrity and availability of data.