RADemics

Anomaly Detection Based on Behavioral Patterns Using AI and Statistical Models

MOHAN PRABHU S, R. Varadharajan
Amity University, SRM Institute of Science and Technology

Anomaly Detection Based on Behavioral Patterns Using AI and Statistical Models

[1]MOHAN PRABHU S, M.Sc., M. Phil., Ph.D., PGDSBSA., Associate Professor of Statistics, Amity School of Applied Sciences, Amity University, Devanahalli - Doddaballapura Road, Bengaluru, Karnataka, India. mprabhu@blr.amity.edu

[2]R. Varadharajan, Associate Professor, Department of Mathematics, College of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur Chengalpattu, Tamil Nadu, India. varadhar@srmist.edu.in

Abstract

The rapid expansion of intelligent digital infrastructures, cloud computing environments, Internet of Things networks, financial transaction platforms, healthcare monitoring systems, and industrial automation technologies has significantly increased the demand for advanced anomaly detection mechanisms capable of identifying abnormal behavioral activities within large-scale dynamic datasets. Traditional rule-based and signature-driven detection approaches demonstrate limited effectiveness against evolving cyber threats, complex operational irregularities, and previously unseen anomalous behaviors due to the absence of adaptive analytical capabilities. Behavioral anomaly detection using Artificial Intelligence and statistical models has therefore emerged as a critical research domain for enhancing system security, operational reliability, predictive intelligence, and real-time decision-making across modern digital ecosystems. This book chapter presents a comprehensive investigation of anomaly detection methodologies based on behavioral patterns through integration of machine learning algorithms, deep learning architectures, probabilistic inference techniques, and statistical analytical frameworks. The chapter examines fundamental concepts of behavioral analytics, contextual behavioral modeling, statistical outlier detection techniques, ensemble learning mechanisms, Generative Adversarial Networks, and multi-level hybrid detection frameworks for intelligent anomaly recognition. Advanced analytical models including Support Vector Machines, Random Forest algorithms, Autoencoders, Long Short-Term Memory networks, Transformer architectures, Bayesian inference systems, and probabilistic behavioral models receive detailed discussion within the context of adaptive anomaly identification across heterogeneous operational environments. Real-time behavioral monitoring, distributed anomaly analytics, privacy-preserving detection systems, explainable Artificial Intelligence, federated learning, and adversarial resilience represent additional focal areas addressed throughout the chapter. Critical research challenges associated with high-dimensional behavioral data, concept drift, data imbalance, scalability limitations, and evolving threat landscapes also receive analytical consideration. The presented discussion establishes a strong conceptual and technological foundation for developing scalable, intelligent, context-aware, and interpretable anomaly detection frameworks suitable for cybersecurity, healthcare, finance, industrial IoT, and smart infrastructure applications within future intelligent computing ecosystems.

Keywords: Behavioral Anomaly Detection, Artificial Intelligence, Statistical Models, Deep Learning, Ensemble Learning, Hybrid Detection Frameworks

Introduction

The rapid growth of intelligent digital technologies, cloud computing platforms, Internet of Things networks, and large-scale communication infrastructures has generated massive volumes of behavioral data across modern computational environments [1]. Such behavioral information contains valuable patterns associated with user activities, operational processes, transaction records, network communications, and system interactions [2]. Increasing dependency on interconnected intelligent systems has significantly elevated security risks, operational uncertainties, and abnormal behavioral activities within digital ecosystems [3,4]. Consequently, anomaly detection based on behavioral analytics has emerged as an essential research area for identifying suspicious activities and preserving system reliability across diverse application domains [5].

Traditional anomaly detection techniques primarily depend upon rule-based mechanisms and predefined attack signatures for identifying abnormal events [6]. Such approaches demonstrate limited adaptability against evolving cyber threats, dynamic behavioral changes, and previously unseen anomalous activities occurring within modern intelligent systems [7]. Static detection frameworks frequently encounter challenges associated with high-dimensional datasets, noisy observations, concept drift, and continuously changing operational conditions [8,9]. Behavioral anomaly detection therefore provides a more adaptive and intelligent analytical framework through continuous monitoring and interpretation of behavioral characteristics [10].