

LEVERAGING BIG DATA FOR REAL-TIME THREAT DETECTION IN ONLINE PLATFORMS

Sreeprasad Govindankutty¹ & Ajay Shriram Kushwaha²

¹*Rochester Institute of Technology, Lomb Memorial Dr, Rochester, NY 14623, United States*

²*Professor, Sharda University, Greater Noida, India*

ABSTRACT

With the rapid proliferation of online platforms, real-time threat detection has become a critical area of focus to ensure user safety and data security. Leveraging big data technologies provides unprecedented opportunities to analyze vast amounts of information in real-time, enabling swift identification and mitigation of potential threats. This paper explores the integration of big data frameworks with advanced analytics and machine learning algorithms to build robust systems for threat detection in online environments.

Key components of this approach include the collection and processing of heterogeneous data sources, such as user behavior logs, transaction records, and social media interactions. These data streams are analyzed in real time using distributed computing frameworks like Apache Hadoop and Spark, ensuring scalability and efficiency. Machine learning models are trained on historical data to detect anomalies, fraudulent activities, and malicious patterns with high accuracy. Moreover, the use of predictive analytics enhances the ability to foresee emerging threats before they materialize.

The proposed approach is evaluated based on its ability to process large-scale data with minimal latency, its adaptability to diverse online platforms, and its precision in identifying threats. Challenges such as data privacy concerns, false positives, and the need for continuous model updates are addressed through secure data processing pipelines and adaptive learning techniques.

This research underscores the transformative potential of big data in safeguarding online ecosystems, providing actionable insights for real-time threat detection, and establishing a resilient defense mechanism for the evolving digital landscape.

KEYWORDS: *Big Data, Real-Time Threat Detection, Online Platforms, Machine Learning, Anomaly Detection, Predictive Analytics, Data Security, Distributed Computing, Cybersecurity, User Behavior Analysis*

Article History

Received: 12 Nov 2024 / **Revised:** 18 Nov 2024 / **Accepted:** 28 Nov 2024
