IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154149

A Severity-Aware Hybrid ML Model for Real-Time Cyber Threat Detection and Alerting

Bhavani Kothapalli[1], Bodapati Preethi[2], Brahma K[3], K P S Kavya[4]

Department of Artificial Intelligence and Machine Learning Ballari Institute of Technology and Management, Karnataka, India[1-4]

Abstract: The increasing dependence on digital authentication systems has increased the risk of unauthorized access and abnormal behavior. Many traditional security systems use fixed rules, which are not effective in detecting new or hidden cyber attacks. This paper presents a severity-aware hybrid machine learning system for real-time cyber threat detection and alerting based on login behavior. The system uses a Random Forest model along with an Isolation Forest model to identify suspicious login activities. Important features such as login time, location, failed attempts, and behavioral patterns are analyzed. Based on the level of risk, the system classifies threats into Low, Medium, and High severity levels. All detected threats are stored and displayed using an interactive dashboard, helping administrators monitor and respond to security issues effectively.

Index Terms: Cybersecurity, Login Behavior Analysis, Anomaly Detection, Machine Learning, Random Forest, Isolation Forest, Severity Classification

I. INTRODUCTION

Login-based authentication systems play a crucial role in protecting modern digital platforms, but they are increasingly targeted by cyber attacks such as brute-force attempts, cre- dential misuse, and suspicious access from unusual locations or devices. Although large amounts of login data are contin- uously generated, identifying which activities are genuinely malicious in real time remains a difficult task. Traditional rule-based security mechanisms rely on fixed thresholds and predefined patterns, making them ineffective against evolving and behavior-driven attacks.

Machine learning has emerged as a powerful approach for analyzing user login behavior and detecting anomalies beyond simple rules. However, methods that rely only on supervised learning depend heavily on labeled attack data, while purely unsupervised techniques often lack contextual understanding and may generate alerts that are difficult to interpret. In addition, many existing systems produce anomaly scores without clearly indicating how severe or risky an event is, limiting their usefulness for security systems.

To overcome these challenges, this paper presents a severity- aware hybrid machine learning approach for real-time cyber threat detection using login behavior analytics. The proposed system combines a Random Forest classifier with an Isolation Forest anomaly detector to capture both known attack patterns and previously unseen behavioral deviations. Login events are analyzed using behavioral, temporal, and contextual features, and a severity scoring mechanism classifies detected activities into Low, Medium, and High risk levels. This severity-based design allows security administrators to prioritize alerts more effectively and respond to potential threats in a timely manner.

II. PROPOSED SYSTEM

The proposed system is designed to detect suspicious login activities in real time by analyzing user authentication behavior using a hybrid machine learning approach. Instead of relying on fixed security rules, the system continuously monitors login events and evaluates them based on behavioral, temporal, and contextual characteristics to identify potential cyber threats.

Login events are collected through a real-time event intake interface and include attributes such as username, source IP address, country, device information, login type, timestamp, and success or failure status. These events are forwarded to a feature engineering module, where meaningful behavioral features are derived. The feature set captures patterns such as recent failed login attempts, changes in access location or IP address, unusual login times, and the time gap between successive logins for a user.

The detection layer of the system employs a hybrid machine learning strategy. A supervised Random Forest classifier is

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154149

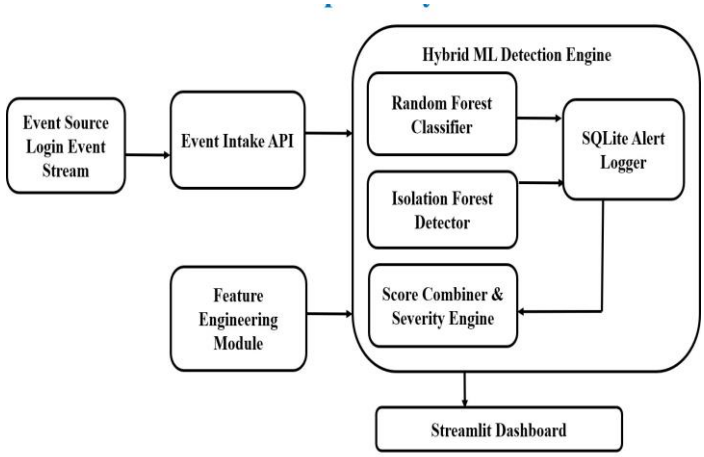

Fig.1 : Architecture Diagram

Fig. 1. Overall architecture of proposed severity-aware cyber threat detection system

used to recognize patterns associated with known malicious behavior based on historical data, while an unsupervised Isolation Forest model detects anomalous login activities that deviate from normal user behavior. By combining these two models, the system was able to identify both previously observed attack patterns and new or unknown threats.

To enhance practical usability, the proposed system includes a severity-aware decision engine. Rather than generating only anomaly scores the engine combines model outputs with contextual rule-based indicators to classify detected events into Low, Medium, and High severity levels. This severity classification helps security administrators prioritize alerts and focus on the most critical threats.

All detected alerts, along with their severity levels and explanations, are stored in a persistent database. An interactive dashboard provides real-time visualization of login activities, alert trends, and geographical access patterns, enabling ef- ficient monitoring and timely response to potential security incidents.

Fig. 1 illustrates the overall architecture of the proposed severity-aware cyber threat detection system. Login events are collected in real time and processed through a feature engi- neering module before being analyzed by a hybrid detection engine combining Random Forest and Isolation Forest models. The resulting risk scores are used by a severity-aware decision module to generate alerts, which are stored and visualized through an interactive dashboard.

III. METHODOLOGY

A. Feature Engineering

Effective feature engineering is critical for accurately mod- eling user login behavior and distinguishing malicious activity from legitimate access patterns. In the proposed system, raw login events are transformed into structured behavioral features that capture temporal, contextual, and historical characteristics of authentication activity.

Each login event includes basic attributes such as username, source IP address, country, device information, login type, timestamp, and success or failure events. These attributes are first normalized to ensure consistency, particularly for categorical fields such as country and device type. Temporal features are then derived from the timestamp, including the login hour, weekend indicator, and identification of unusual access times.

To capture short-term and long-term behavioral patterns, the system computes rolling statistics over recent login history for each user. This includes the number of failed login attempts within predefined time windows, the time elapsed since the previous login, and indicators of changes in access context such as new IP addresses or new geographical locations. These features are effective in identifying brute-force attempts, credential misuse, and anomalous access behavior.

In addition, contextual risk information is incorporated by assigning risk scores to countries based on predefined threat intelligence. Categorical features such as username and country are encoded into numerical representations to ensure compatibility with machine learning models. The resulting feature vector provides a compact yet expressive representation of each login event, enabling robust behavioral analysis by the detection models.

B. Hybrid Detection Model

The proposed system employs a hybrid machine learning detection strategy that combines supervised and unsupervised models to improve robustness against diverse cyber threat pat- terns. Relying on a single learning paradigm can be limiting, as supervised models depend on labeled attack data, while unsupervised models may lack contextual

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026
DOI: 10.17148/IJARCCE.2026.154149

understanding. By integrating both approaches, the system is able to detect known attack behaviors as well as previously unseen anomalies.

A supervised Random Forest classifier is used to analyze login events based on historical behavioral patterns. The model learns complex decision boundaries from labeled data and pro- duces a probability score indicating the likelihood of malicious activity. Random Forest is well suited for this task due to its ability to handle heterogeneous features, reduce overfitting, and provide stable predictions in noisy environments.

In parallel, an unsupervised Isolation Forest model is used to detect anomalous login behavior by measuring how easily an event can be isolated from normal patterns. Login events that significantly deviate from typical user behavior are assigned higher anomaly scores. This enables the system to identify novel or rare attack patterns that may not be present in labeling training data.

The outputs of both models are combined to generate a unified threat score for each login event. By leveraging the complementary strengths of supervised classification and unsupervised anomaly detection, the hybrid model achieves improved detection accuracy and resilience against evolving cyber threats

C. Severity Classification

While anomaly scores provide useful indicators of suspi- cious behavior, they do not directly convey the level of risk associated with a login event. To address this limitation, the proposed system incorporates a severity-aware classification mechanism that translates detection outcomes into actionable risk levels. This enables security administrators to prioritize alerts and respond more effectively to potential threats.

The severity classification module combines the outputs of the hybrid detection model with contextual rule-based

indicators derived from login behavior. Factors such as re- peated failed login attempts, access from new geographical locations or IP addresses, and login occurring at unusual times are considered when determining severity. These indicators provide additional context that enhances the interpretability of machine learning outputs.

Based on the combined threat score and contextual indica- tors, each login event is classified into one of three severity levels: Low, Medium, or High. High-severity alerts correspond to strong indicators of compromise and require immediate attention, while medium-severity alerts represent suspicious behavior that may warrant monitoring. Low-severity events typically reflect benign deviations from normal behavior and are retained for audit purposes.

By integrating machine learning predictions with severity- aware decision logic, the proposed approach improves the operational usability of anomaly detection and reduces alert fatigue. This classification strategy ensures that critical threats are highlighted promptly while maintaining visibility into lower-risk activities.

IV. RESULTS AND DISCUSSION

The proposed severity-aware hybrid machine learning sys- tem was evaluated using a stream of login events designed to represent both normal user behavior and malicious access pat- terns. The evaluation focused on the system's ability to detect anomalous login activity, classify threat severity accurately, and provide meaningful alerts in real time.

Experimental observations indicate that the hybrid detection approach improves robustness compared to using a single model. The Random Forest classifier effectively identifies known attack patterns such as repeated failed login attempts, while the Isolation Forest model successfully detects unusual login behavior that deviates from historical norms. By combin- ing both models, the system is able to detect both previously observed and novel attack scenarios.

The severity classification mechanism further enhances the practical usefulness of the detection system. High-severity alerts are generated for login events exhibiting strong in- dicators of compromise, such as rapid consecutive failures or access from new geographical locations. Medium-severity alerts capture suspicious but less critical behavior, while low- severity events represent minor deviations that are useful for audit and trend analysis. This prioritization helps reduce alert fatigue and allows security administrators to focus on the most critical threats.

The interactive dashboard provides real-time visibility into detected threats, severity distribution, and geographical access patterns. This visualization capability supports efficient mon- itoring and improves situational awareness, enabling timely investigation and response to potential security incidents. Overall, the results demonstrate that the proposed severity- aware hybrid approach is effective, interpretable, and suitable for real-world cybersecurity monitoring environments.

CONCLUSION

This paper presented a severity-aware hybrid machine learn- ing framework for real-time cyber threat detection based on login behavior analysis. By combining a supervised Random Forest classifier with an unsupervised Isolation Forest

DOI: 10.17148/IJARCCE.2026.154149

anomaly detector, the proposed system effectively identifies both known attack patterns and previously unseen anomalous behavior. The integration of behavioral feature engineering and severity- aware decision logic enables meaningful classification of threats into Low, Medium, and High risk levels.

The proposed approach improves the interpretability and op- erational usefulness of anomaly detection by prioritizing alerts based on severity, thereby reducing alert fatigue and supporting timely security response. Experimental observations demon- strate that the system is suitable for real-time deployment and provides efficient monitoring through an interactive dashboard. Future work may focus on integrating the system with large- scale security information and event management platforms, incorporating deep learning-based models for enhanced behav- ioral analysis, and extending support to multi-source log data from network, cloud, and endpoint environments.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to Mrs. Kavya Sree K, Assistant Professor, Department of Artificial Intelligence and Machine Learning, Ballari Institute of Technology and Management, for her valuable guidance, continuous support, and encouragement throughout the course of this research work. The authors also thank Mrs. P. Asha Jyothi, Assistant Professor and Project Coordinator, for her coordination and constructive suggestions. The authors are grateful to Dr. B. M. Vidyavathi, Professor and HOD, Depart- ment of Artificial Intelligence and Machine Learning, for her support and motivation. The authors also acknowledge Ballari Institute of Technology and Management for providing the necessary infrastructure and academic environment to carry out this research.

REFERENCES

[1] L. Breiman, “Random forests,” *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.
[2] F. T. Liu, K. M. Ting, and Z.-H. Zhou, “Isolation forest,” in *Proc. IEEE Int. Conf. Data Mining (ICDM)*, Pisa, Italy, 2008, pp. 413–422.
[3] A. Patcha and J.-M. Park, “An overview of anomaly detection techniques: Existing solutions and latest technological trends,” *Computer Networks*, vol. 51, no. 12, pp. 3448–3470, 2007.
[4] S. Axelsson, “Intrusion detection systems: A survey and taxonomy,” Tech. Rep., Chalmers Univ. Technology, Sweden, 2000.
[5] Y. Bengio, A. Courville, and P. Vincent, “Representation learning: A review and new perspectives,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 35, no. 8, pp. 1798–1828, 2013.
[6] A. Lazarevic, L. Ertoz, V. Kumar, A. Ozgur, and J. Srivastava, “A comparative study of anomaly detection schemes in network intrusion detection,” in *Proc. SIAM Int. Conf. Data Mining*, 2003, pp. 25–36.
[7] S. Dua and X. Du, *Data Mining and Machine Learning in Cybersecurity*. Boca Raton, FL, USA: CRC Press, 2016.
[8] R. Sommer and V. Paxson, “Outside the closed world: On using machine learning for network intrusion detection,” in *Proc. IEEE Symp. Security and Privacy*, Oakland, CA, USA, 2010, pp. 305–316.
[9] M. Ahmed, A. N. Mahmood, and J. Hu, “A survey of network anomaly detection techniques,” *J. Netw. Comput. Appl.*, vol. 60, pp. 19–31, 2016.
[10] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.
[11] O. Mykhaylova, A. Shtypka, and T. Fedynyshyn, “An Isolation Forest-based approach for brute force attack detection,” in *CEUR Workshop Proc.*, vol. 3842, 2024.
[12] I. A. Igbaria and E. Mahmoud, “IFDRF: A hybrid Isolation Forest and Random Forest model for anomaly detection,” *Optical Memory and Neural Networks*, vol. 34, no. 7, pp. 533–546, 2025.
[13] E. Cambria, S. Poria, and D. Hazarika, “Explainable artificial intelligence for cybersecurity applications,” *Frontiers in Artificial Intelligence*, vol. 8, 2025.

