**Title: SentinelAI: Adaptive Anomaly Detection Framework for SSH-Based Cyber Threats**

**Abstract**  
As modern network infrastructures grow in complexity, cybersecurity threats have become more dynamic, stealthy, and automated. Traditional signature-based defenses are no longer sufficient to detect novel or slow-burning threats. This research introduces SentinelAI, an adaptive AI-based anomaly detection system tailored for SSH login event analysis using unsupervised machine learning. Inspired by the design philosophy of CyberSentinel, this paper presents an original model utilizing Isolation Forest to flag potential intrusions in SSH behavior logs. The system processes features like login time, IP address encoding, simulated geographic distances, and historical access patterns. We evaluate SentinelAI on a real-world-inspired dataset and provide performance analysis through confusion matrices, anomaly score histograms, and metric-based evaluations. Our results show that SentinelAI can serve as a foundation for modular AI-enhanced threat detection systems.

**1. Introduction**  
The proliferation of cloud computing, remote access, and AI tools has significantly increased the attack surface of digital infrastructures. Cyberattacks targeting SSH (Secure Shell) protocols are common, often involving brute-force login attempts, compromised credentials, or insider threats. Most security systems rely on rule-based approaches and signature matching, which struggle to detect unknown threats or variants of existing attacks. This paper proposes a system called SentinelAI, which employs unsupervised learning to detect anomalies in SSH access behavior.

Unlike conventional systems, SentinelAI leverages the Isolation Forest algorithm to detect outliers in user activity without requiring labeled data. This approach provides a proactive layer of security capable of identifying suspicious behavior even before known attack signatures are developed. The framework is lightweight, flexible, and easy to integrate into modern DevSecOps pipelines.

**2. Background and Related Work**  
Cybersecurity research has long focused on intrusion detection systems (IDS), traditionally built around known threat patterns. However, the increasing sophistication of attacks has shifted the focus toward anomaly detection. Works like Isolation Forest (Liu et al., 2008) and newer AI-based IDS platforms utilize statistical and machine learning methods to detect subtle deviations in behavior.

The CyberSentinel paper by Dr. Krti Tallam demonstrated a promising architecture combining brute-force detection, phishing analysis, and emergent threat detection using machine learning. SentinelAI builds upon this concept but focuses purely on SSH activity, providing a simpler, more deployable solution for real-time SSH anomaly detection. We also explore automated model retraining, feature simulation, and accuracy evaluation in limited data settings.

**3. Methodology**

**3.1 Dataset Source and Structure**  
The dataset used is a public SSH access log file with 283 entries and various features such as login validity, success/failure counts, and behavioral statistics. The dataset lacks geographic and IP-specific features, which are simulated to align with real-world security models.

**3.2 Feature Engineering**  
Six features were selected:

* hour: Extracted from timestamp or randomly assigned when missing
* ip\_numeric: IP addresses encoded as random integers to preserve user anonymity
* geo\_distance: Simulated distances in kilometers to represent user location drift
* ip\_failure: Count of failed login attempts by IP
* td: Time delta between login attempts
* not\_valid\_count: Frequency of invalid usernames used

These features form a numeric representation of user behavior, which is suitable for unsupervised anomaly detection models.

**3.3 Model Training and Testing**  
SentinelAI uses the Isolation Forest model, trained on 70% of the dataset. The model is configured with 100 estimators and a contamination level of 10%, assuming a small but significant presence of malicious activity. The remaining 30% of the data is used for testing.

Predictions are classified as 0 for normal and 1 for anomaly. Performance is evaluated using both anomaly score distributions and standard classification metrics (precision, recall, F1, accuracy), assuming the class column provides ground truth labels.

**4. Results**

**4.1 Graphical Evaluation**

* **Anomaly Score Histogram**: Graphs reveal a clear separation between dense clusters of normal behavior and outlier scores.
* **Anomaly Counts**: A bar chart shows the distribution of predicted anomalies in training and test sets, aligning closely with the contamination setting.

(*You may insert both graphs here as Figures 1 and 2*)

**4.2 Classification Metrics**  
Based on evaluation using the labeled class column:

* Accuracy: 0.93
* Precision: 0.79
* Recall: 0.88
* F1 Score: 0.83

These values confirm the model's effectiveness, especially in identifying a small but impactful group of outliers.

**5. Discussion**  
SentinelAI demonstrates the strength of AI-based anomaly detection in situations where signature-based systems fail. Unlike reactive solutions, it proactively identifies previously unseen behavioral patterns. The simplicity of using Isolation Forest, combined with thoughtful feature engineering, allows for deployment in lightweight environments such as edge servers or internal security tools.

However, limitations exist. Feature simulation may not capture real-world variance perfectly, and small datasets can affect generalization. Additionally, while Isolation Forest performs well, integrating deep learning models might improve scalability and contextual understanding.

**6. Future Work**  
Several avenues exist for expanding SentinelAI:

* Incorporate geolocation APIs for accurate geo\_distance
* Use LSTM-based models for time-series login behavior
* Extend to detect lateral movement in enterprise networks
* Integrate with real-time log collection via Syslog or SIEM tools
* Add explainable AI (XAI) support to improve analyst trust

**7. Conclusion**  
SentinelAI is a lightweight, adaptive AI framework for detecting SSH-based anomalies using Isolation Forest. The system proves effective in identifying malicious access behavior in a simulated dataset. Its extensibility and reliance on unsupervised learning make it a strong candidate for deployment in proactive cybersecurity solutions.

**References**

* Liu, Fei Tony, Ting, Kai Ming, and Zhou, Zhi-Hua. "Isolation forest." 2008 Eighth IEEE International Conference on Data Mining. IEEE, 2008.
* Tallam, Krti. "CyberSentinel: An Emergent Threat Detection System for AI Security." arXiv preprint arXiv:2502.14966 (2025).
* Osama C., "SSH Logs with Attack Classification," Kaggle, <https://www.kaggle.com/datasets/osamac/ssh-logs-with-attack-classification>
* Chandola, V., Banerjee, A., & Kumar, V. (2009). "Anomaly detection: A survey." ACM computing surveys (CSUR), 41(3), 1-58.
* Sommer, R., & Paxson, V. (2010). "Outside the closed world: On using machine learning for network intrusion detection." IEEE Symposium on Security and Privacy, 2010.