IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Smart Intrusion Detection System: Hybrid AI/ML Intrusion Detection for Cloud Environments with Real-Time Security Analytics

1st AnushShetty
Department of Electronics and Computer Science Shah and Anchor Kutchhi Engineering College Chembur, Mumbai, India

2nd Rahul Budhani
Department of Electronics and Computer Science Shah and Anchor Kutchhi Engineering College Chembur, Mumbai, India

3rd Abhishek Kolkar
Department of Electronics and Computer Science Shah and Anchor Kutchhi Engineering College Chembur, Mumbai, India

4th Yash Bhosale
Department of Electronics and Computer Science Shah and Anchor Kutchhi Engineering College Chembur, Mumbai, India

5th Dr. Pramod Bhavarthe
Department of Electronics and Computer Science Shah and Anchor Kutchhi Engineering College Chembur, Mumbai, India

Abstract—Cloud-hosted applications continue to face sophisti- cated threats including brute-force attacks, automated scraping, malicious query execution, insider misuse, and unauthorized data extraction. Conventional intrusion detection systems generally de- pend on either static rule signatures or isolated machine learning models, often resulting in limited adaptability or poor explain- ability. This paper presents Smart IDS, a hybrid AI/ML intrusion detection framework designed for cloud environments with real- time security analytics. The proposed system combines deter- ministic threat heuristics with Isolation Forest based anomaly detection to identify both known and unknown attack behavior. A weighted risk scoring model dynamically categorizes incidents into operational severity tiers. To reduce analyst workload, a locally deployed large language model generates concise incident summaries and immediate mitigation guidance for severe alerts. The platform also includes a live dashboard for monitoring traffic anomalies, risk trends, geographic attack sources, and active alerts. Experimental observations demonstrate improved detec- tion accuracy, faster triage capability, and privacy- preserving automated incident response suitable for modern cloud security operations.

Index Terms—Cloud Security, Intrusion Detection System, Artificial Intelligence, Machine Learning, Isolation Forest, Real- Time Analytics, Cybersecurity

I. INTRODUCTION

Cloud computing has emerged as an important compo- nent of modern-day technology. Cloud computing enables deployment of scalable applications, database management for dispersed databases, provision of virtual services, and collaboration in remote areas with reduced costs. Private clouds, public clouds, and hybrid clouds have been adopted by many institutions ranging from the financial sector, health care institutions, education, manufacturing industries, to gov- ernment institutions owing to their cost-effective nature. But while these qualities make cloud computing appealing, the same qualities also give rise to cybersecurity problems.

As compared to on-premises networks, cloud infrastructure offers its services via web-based API endpoints, web inter- faces, remote management applications, and interconnected microservices. Attacks on cloud infrastructure can be car- ried out by means of techniques such as credential stuffing, brute force login attacks, privilege escalation, malicious query injections, recon probes, malicious insider use, and illicit data extraction from cloud workloads. In addition to this, cloud workloads generate vast amounts of data related to authentications, accesses, and transactions. It is difficult for security professionals to detect any potential threats through manual surveillance. Therefore, intrusion detection systems (IDS) continue to remain among the most crucial technologies for threat hunting. Traditional IDS systems usually have two approaches: signature-based systems and anomaly-based sys- tems. Signature-based systems are useful in detecting known types of attacks that are characterized by a particular pattern. However, their inability to detect rapidly evolving attacks makes signature-based systems inefficient.

Meanwhile, anomaly-based IDS relies on statistical and machine learning approaches. These IDS systems are capable of detecting newly developed attacks; however, they produce many false alerts due to complex user behavior.

Advancements in artificial intelligence and machine learning

technologies have contributed towards flexible approaches in security. Supervised and unsupervised learning models are capable of studying behavioral patterns, categorizing malicious traffic, and identifying hidden anomalies. Moreover, Large Language Models can aid in summarization, reasoning, and process optimization. Within the realm of cybersecurity operations, these capabilities can help reduce the burden of analysts in generating justifications for threats and providing recommendations. Nonetheless, most modern AI-enabled solutions rely on third-party cloud APIs, causing latency, and legal issues when confidential security logs should be exchanged externally.

To address these challenges, this paper proposes a Smart IDS approach that consists of a hybrid artificial intelligence (AI)/machine learning (ML) intrusion detection system for cloud environments with real-time security analytics capabili- ties. It combines rule-based and ML models of threat detection to improve efficiency in detecting and identifying the attack types for both known and unknown attack scenarios. With the help of a special algorithm that determines weighted threat scoring, the detected events are sorted based on the severity level. In case of critical alert generation, incident summary and recommendations for action taken with the Large Language Model deployed in a local environment are produced, while sensitive information is not shared with any external parties. In the proposed smart IDS solution, there is a real-time dashboard available with visual representations of the incidents detected. The security officers are provided with the necessary tools for monitoring changes in risk levels, alerts opened, anomalies distribution, geographical location of attacks, among other im- portant metrics. Technical effectiveness and user-friendliness of the solution are achieved because of the use of hybrid detection, local AI solutions, and visualization.

Some of the contributions of the suggested framework include development of a hybrid intrusion detection system combining a rule-based one with ML algorithms, application of weighted scoring method to determine severity level of incidents, implementation of a local language model to provide recommendations on handling incidents, creation of real-time cloud security analytics dashboard, and light-weight architec- ture.

II. RELATEDWORK

Although there is a high adoption of rule-based methods such as Snort in detecting known signatures, these are expen- sive in terms of rule updating and ineffective against unknown threats. Statistical methods try to find anomalies within traffic but generate too many false alarms in dynamic environments. Supervised and unsupervised learning techniques have been utilized for intrusion detection. Among these approaches, the isolation forest algorithm is highly effective in finding infrequent anomalies because it runs faster and uses fewer resources. Deep learning can provide higher accuracy results, but more samples and expensive hardware are required.

Recent developments in cyber security involve the utiliza- tion of generative AI for analyzing data and generating reports. However, most of these applications rely on external API services that raise confidentiality concerns. On the contrary, Smart IDS stands out due to its hybrid approach along with an internal language model.

III. SYSTEM ARCHITECTURE

An intelligent Intrusion Detection System uses a modular layered approach consisting of the ingestion, detection, intel- ligence, storage, and visualization layers.

A. Frontend Layer

The frontend was developed using React.js and Vite frame- work. The Recharts library can be used for graph rendering, while responsive images. Updates made to the dashboard periodically without full page reload.

B. Backend Layer

The backend layer consists of fast API that provides the REST interface while SQLAlchemy acts as a database man- ager. It handles the analysis and scoring process.

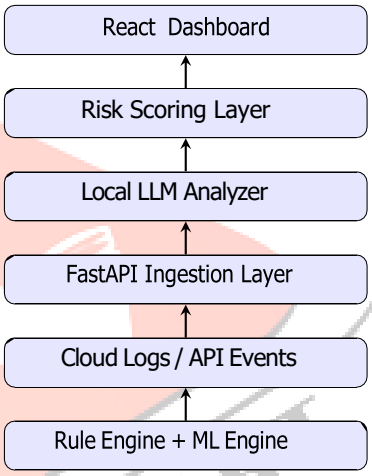

Fig. 1. Smart IDS layered architecture

IV. DETECTIONMETHODOLOGY

Each incoming log passes through two levels of detection algorithms.

A. Rule-Based Heuristics

The immediate danger signs are classified based on rules provided in Table I.

TABLEI
RULE -BASED THREAT SCORING

Condition	Score
Failed logins > 5	+60
Download > 100 MB	+50
DROP / DELETE query	+40
Query count > 100	+30
Honeypot table access	+100

B. Machine Learning Model

Isolation Forest algorithm is trained using the baseline dataset of traffic data with three key features:

- Query count
- Failed login attempts •

Download size (MB)

C. Risk Fusion Model

The formula used to calculate the risk score is as follows:

$$R = 0.7 \cdot S_r + 0.3 \cdot S_m \quad (1)$$

where S_r refers to rule score, and S_m is the machine learning anomaly score. Levels of Severity:

- Low–if$R<30$
- Medium–if$30 \leq R<60$
- High–if$60 \leq R<80$
- Critical – if $R \geq 80$

V. AI INCIDENT INTELLIGENCE

In the event that the threat categorization is either High or Critical, Smart IDS will utilize the Mistral model running locally through Ollama. It will prompt the model to behave like a SOC analyst, generating a summary that includes:

- Predicted threat behavior
- Operational risks
- Two mitigating actions

VI. EXPERIMENTALSETUP

The testing process involved artificial cloud logs that mim- icked both legitimate actions and attacks. The attacks simu- lated were:

- Failed-login floods
- Destructive SQL queries
- Scraper floods
- Massive downloads
- Attempts to access honeypots

Metrics for assessing performance were accuracy, precision, recall, false positives, and response time.

VII. RESULTS AND DISCUSSION

A. Detection Accuracy

Combination of both deterministic and behavioral intelli- gence was effective in the hybrid model compared to individ- ual techniques.

B. Distribution of Threat Severity

C. Risk Trend Tracking

From the results above, it is evident that Smart IDS main- tains detection efficiency without being too heavy.

VIII. SECURITY AND PRIVACY CONSIDERATIONS

As opposed to cloud-based AI, Smart IDS does incident summarization on-premises. This ensures that any confidential data is not sent out of the company premises. The API calls can be authenticated, encrypted, and logged for compliance purposes within the enterprise environment.

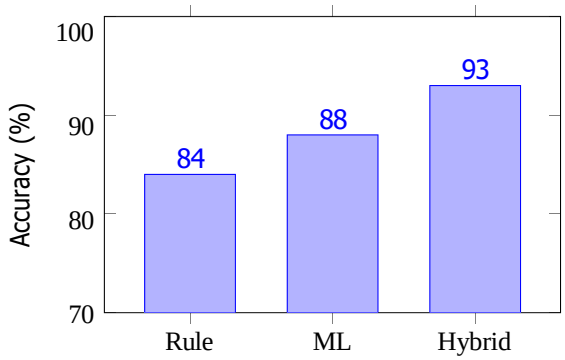

Fig. 2. Accuracy comparison of detection models

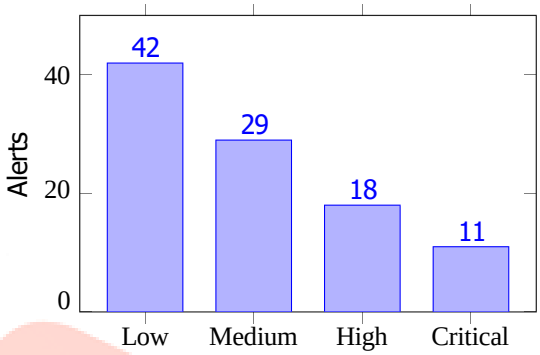

Fig. 3. Observed alert severity distribution

IX. LIMITATIONSANDFUTUREWORK

Although efficient, the existing prototype of the system has the following drawbacks:

- The use of synthetically generated test data instead of traffic data from the corporation
- TheuseofpollingdashboardinsteadofWebSocket-based stream
- Insufficient number of anomalies detection features Some future improvements may involve:
- Federated learning among several cloud nodes
- Deep sequences for traffic analysis
- SIEM integration
- Containment playbooks
- Threshold optimization

X. CONCLUSION

This paper brought forth Smart IDS – an AI/ML hybrid intrusion detection solution to cloud environment security based on real-time analytics. The combination of deterministic methods, Isolation Forest learning, threat assessment, and investigation through local language models made sure that the solution remained explainable and adaptive to detect any potential threats. The results of the empirical study revealed that hybrid solutions could significantly enhance the cloud security without breaching privacy policy norms and causing additional burden.

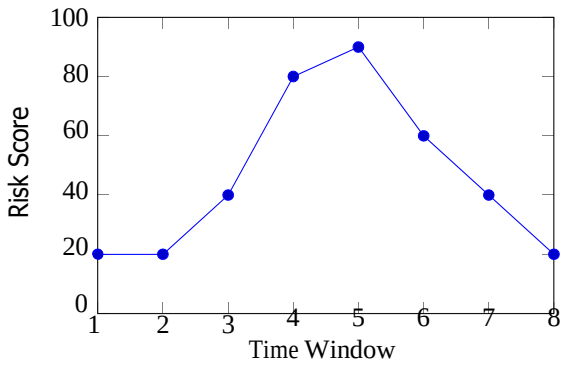

Fig. 4. Real-time dashboard risk trend

TABLE II
PERFORMANCE METRICS

Metric	Value
Accuracy	93.4%
Precision	91.2%
Recall	89.8%
False Positive Rate	6.1%
API Response Time	210 ms 1.8s
LLM Summary Time	2 s
Dashboard Refresh	

REFERENCES

[1] F. T. Liu, K. Ting, and Z. Zhou, “Isolation Forest,” IEEE ICDM, 2008. [2] R. Sommer and V. Paxson, “Outside the closed world: machine learning for intrusion detection,” IEEE Security and Privacy, 2010.

[3] W.LeeandS.Stolfo,“Dataminingapproachesforintrusiondetection,” USENIX, 1998.

[4] Snort Project, “Snort IDS/IPS Documentation,” 2025.

[5] OWASP Foundation, “Cloud Security Top Risks,” 2025.

[6] FastAPI Documentation, “Modern Python APIs,” 2025.

[7] Scikit-learn Documentation, “IsolationForest,” 2025.

[8] Mistral AI, “Open-weight language models,” 2025.

[9] NIST, “Guide to Intrusion Detection and Prevention Systems,” 2024.

[10] ENISA, “Cloud Threat Landscape Report,” 2025.