AI-Driven Cybersecurity Framework for Energy Research Infrastructure and Geoscience Data Systems

[1]*M. Abouawn*
[1]*Petroleum Research Centre- Tripoli, Libya,*
email: m.abouawn@prclibya.com
ORCID No.0009-0007-2736-978X

Abstract

This study aims to design, evaluate, and validate an AI-driven cybersecurity framework tailored specifically for energy research infrastructures and geoscience data systems operating mission-critical scientific workloads. Artificial Intelligence (AI) has become essential to strengthening cybersecurity in national energy research environments that host sensitive geoscience workloads. The proposed framework correlates machine-learning–based anomaly detection with identity, endpoint, and network telemetry to surface early-stage attack signals. The evaluation combines operational metrics from production geoscience servers with internal detection benchmarks derived from Microsoft security platforms in the institutional environment. Production telemetry reports 12 restart cycles per year, zero unplanned technical outages, no security-incident downtime, and 168 annual downtime hours—equating to 98.08% availability. Across controlled detection exercises, the AI layer reduced Mean Time to Detect (MTTD) by approximately 30% relative to the historical triage baseline while improving endpoint-compliance visibility. These results highlight the value of integrating AI analytics with existing controls to harden geoscience data systems and mission-critical research services in national energy institutions.

Keywords - Artificial Intelligence, Anomaly Detection, Cybersecurity, Energy Infrastructure, Geoscience Data Protection.

إطار عمل للأمن السيبراني قائم على الذكاء الاصطناعي لحماية البنى التحتية لأبحاث الطاقة وأنظمة بيانات علوم الأرض

مروة أبوعون
مركز بحوث النفط

الملخص

تهدف هذه الدراسة إلى تصميم وتقييم والتحقق من صحة إطار للأمن السيبراني مدعوم بالذكاء الاصطناعي، ومصمم خصيصاً للبنى التحتية لأبحاث الطاقة وأنظمة بيانات علوم الأرض التي تشغّل أحمالاً علمية حرجة .أصبح الذكاء الاصطناعي عنصراً مهماً في تعزيز الأمن السيبراني في بيئات أبحاث الطاقة الوطنية التي تستضيف أحمالاً حساسة لعلوم الأرض .ويعمل الإطار المقترح على ربط اكتشاف الشذوذ القائم على التعلم الآلي مع بيانات الهوية ونقاط النهاية وحركة الشبكة للكشف المبكر عن مؤشرات الهجمات .ويجمع التقييم بين مقاييس تشغيلية لخوادم علوم الأرض المستخدمة في بيئة الإنتاج ومعايير داخلية للكشف مستمدة من منصات Microsoft الأمنية في البيئة المؤسسية .وتُظهر بيانات التشغيل 12 دورة إعادة تشغيل سنوياً، وعدم وجود أعطال تقنية غير مخططة، وعدم وجود توقف ناتج عن حوادث أمنية، و 168ساعة توقف سنوياً، بما يعادل توافراً قدره 98.08%. وفي اختبارات كشف مضبوطة، خفّضت طبقة الذكاء الاصطناعي متوسط زمن اكتشاف الحوادث (MTTD)بنحو 30% مقارنة بخط الأساس للفرز التاريخي، مع تحسين وضوح امتثال نقاط النهاية .وتبرز هذه النتائج قيمة دمج تحليلات الذكاء الاصطناعي مع الضوابط القائمة لتعزيز حماية أنظمة بيانات علوم الأرض وخدمات الأبحاث الحرجة في مؤسسات الطاقة الوطنية.

الكلمات المفتاحية: الذكاء الاصطناعي، اكتشاف الشذوذ، الأمن السيبراني، البنية التحتية للطاقة، حماية بيانات علوم الأرض

1. Iintroductions

The rapid digitalization of the energy sector has significantly increased reliance on high-performance computing (HPC), cloud-based identity services, and interconnected research networks that process large and sensitive scientific datasets. Energy research institutions engaged in petroleum exploration, renewable energy modelling, and subsurface analysis operate specialized geoscience servers for seismic processing, reservoir simulation, and geological computations that support scientific research and strategic decision-making.

Energy research infrastructure represents a critical component of modern scientific and industrial development. As these environments increasingly rely on digital platforms and connected systems, cybersecurity has become an essential requirement to ensure the reliability and integrity of research operations. As digital infrastructures expand across research environments, the organizational attack surface grows accordingly, exposing institutions to cybersecurity risks including unauthorized access, malware intrusion, lateral movement, and data exfiltration. At the same time, the growing adoption of Artificial Intelligence (AI) technologies across the energy sector introduces both new operational opportunities and additional security challenges that must be addressed in order to protect critical digital assets and scientific data platforms (Bishop, 2018).

Traditional cybersecurity monitoring systems have historically relied on rule-based and signature-based detection techniques to identify malicious activity. While these approaches remain effective for detecting known indicators of compromise, they often struggle to identify sophisticated attacks, previously unseen threat patterns, or subtle insider behaviors. In modern research infrastructures, the volume and diversity of security telemetry—including identity authentication logs, endpoint security events, and internal network traffic—continue to grow rapidly. This increasing complexity frequently exceeds the capacity of manual analysis and can significantly increase the Mean Time to Detect (MTTD) security incidents in large-scale research environments.

Artificial Intelligence-assisted security monitoring provides a promising approach for addressing these challenges. Machine learning algorithms can analyze heterogeneous security data sources, identify behavioral anomalies, and detect abnormal activity patterns that may indicate emerging cyber threats. By correlating identity events, endpoint telemetry, and network traffic data, AI-driven cybersecurity systems can enhance early threat detection while reducing the workload of security analysts. These capabilities are particularly important in research environments where large scientific datasets and distributed computing resources require continuous monitoring and protection.

Operational observations from institutional network monitoring further illustrate the complexity of traffic behavior within research infrastructures. Firewall telemetry indicates frequent blocked connection attempts, detectable proxy or VPN usage, and high volumes of traffic within categories such as social networking platforms. These traffic patterns may increase the potential risk of unauthorized

access or covert data movement if not properly monitored. Consequently, advanced security analytics including machine learning-based anomaly detection and user behavior analysis become essential tools for strengthening monitoring capabilities in complex research networks (Liu et al., 2008).

The objective of this study is to propose, evaluate, and validate an AI-driven cybersecurity framework tailored specifically for energy research infrastructures by correlating identity, endpoint, and network telemetry to improve anomaly detection capabilities. Furthermore, this study presents an operational reliability snapshot of geoscience computing servers—including system restarts, downtime events, and infrastructure availability metrics—to establish a baseline for secure research operations, while evaluating observed improvements in detection efficiency, including an approximate 30% reduction in Mean Time to Detect (MTTD) achieved within the research environment.

2. Literature Review

Traditional intrusion detection systems (IDS) have long relied on rule-based and signature-based mechanisms, which remain effective for known threats but struggle to detect low-frequency or previously unseen attacks due to the base-rate fallacy (Axelsson, 2000). Early cybersecurity literature established foundational security principles and access-control models for protecting digital environments (Bishop, 2018), while subsequent advances in machine learning expanded detection capabilities to include automated analysis of complex security telemetry (Aggarwal, 2019). Machine-learning-driven anomaly detection has become widely adopted in modern cybersecurity frameworks. Algorithms such as Isolation Forest have shown strong performance in identifying anomalous behavior in high-dimensional datasets (Liu et al., 2008), whereas supervised models including Random Forest and XGBoost have demonstrated high accuracy in classifying attack patterns (Buczak and Guven, 2016; Chen and Guestrin, 2016). Deep-learning-based intrusion detection approaches have also improved detection of sophisticated threats, particularly in network-centric environments (Javaid et al., 2016; Berman et al., 2019).

Industry and research guidelines emphasize multi-layered monitoring across identity, endpoint, and network channels. NIST SP 800-94 highlights the importance of integrating data from multiple security domains to improve detection fidelity (NIST, 2007), while modern enterprise architectures such as Microsoft Defender and XDR platforms promote identity-centric and endpoint-driven threat visibility (Microsoft Security, 2024). Benchmark datasets such as UNSW-NB15 continue to support the evaluation of machine-learning-based intrusion detection systems (Moustafa and Slay, 2015).

Despite these advancements, existing AI-based cybersecurity frameworks rarely address the unique operational and technical requirements of geoscience computing environments, which combine high-value subsurface datasets, high-performance computing (HPC) workloads, and heterogeneous telemetry sources. Current approaches seldom integrate identity, endpoint, and network data into a unified AI-driven model designed specifically for energy research

infrastructures, leaving a critical gap that this work aims to address.

3. Methodology

3.1 Telemetry Acquisition

Security telemetry was collected over a six-month monitoring period from four primary sources within the research environment:

1. Microsoft Entra ID authentication logs — capturing login failures, off-hours access, and location anomalies.
2. Microsoft Defender for Endpoint/XDR — providing process-creation activity and endpoint security signals.
3. Geoscience server audit logs — reflecting HPC workloads, storage I/O, and dataset access operations.
4. FortiGate firewall logs — representing east-west traffic patterns and outbound communication behaviour.

These sources cover the full attack surface typical of energy and geoscience infrastructures.

3.2 Data Processing and Feature Engineering

Telemetry from all sources was normalized into a unified schema and aggregated into short time windows to stabilize behaviour. Preprocessing steps included timestamp alignment, deduplication, and handling of missing values.

A compact feature set was engineered to capture key security-relevant behaviours:

- Identity-level features: login fail ratio, off-hours authentication, new location login.
- Endpoint-level features: process spawn rate, unsigned binary execution.
- Network-level features: east-west fan-out, outbound egress spikes.
- Server-level features: storage I/O spikes, abnormal dataset access frequency.

These features were selected because they directly reflect common early-stage attack patterns observed in operational environments such as credential misuse and lateral movement.

Table 1. Key Security Features Extracted from Telemetry

Feature Category	Example Indicators	Source
Identity	Login fail rate, off-hours login	Entra ID
Endpoint	Process spawn rate, unsigned binaries	Defender XDR
Network	East-west fan-out, egress spikes	Firewall
Geoscience Servers	I/O volume spikes, unusual dataset access	Server logs

3.3 Hybrid AI-Based Detection Framework

The detection component integrates both unsupervised and supervised machine-learning algorithms to identify unknown threats and classify known attack behaviours.

- Unsupervised anomaly detection: Isolation Forest was used to learn baseline behavior across telemetry streams and flag deviations indicative of potential threats.
- Supervised classification: Models such as Random Forest and XGBoost were applied to detect known attack types based on labeled historical patterns. This hybrid approach improves sensitivity to subtle identity anomalies, lateral movement behaviors, endpoint irregularities, and high-volume geoscience-data access. The final detection output is sent to enterprise SIEM/XDR systems for automated alerting and response as shown in Figure 1.

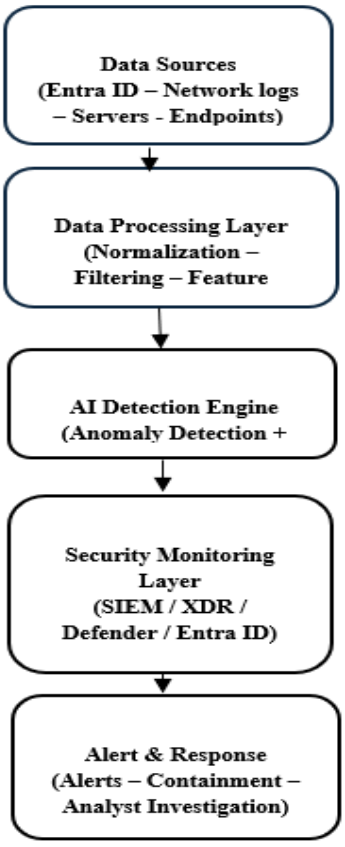


Figure 1 Proposed AI-Driven Cybersecurity Framework Architecture

4. Evaluation Metrics

The effectiveness of the proposed AI-driven cybersecurity framework is evaluated using several standard performance metrics commonly used in intrusion detection and security analytics. These metrics include precision, recall, F1-score, ROC-AUC, alert volume per day, investigation yield, and Mean Time to Detect (MTTD).

To assess system reliability, annual availability is calculated using the following equation:

$$\text{Availability} = \frac{8760 - \text{Downtime(h)}}{8760} \times 100 \quad (1)$$

Availability equation

where 8760 represents the total number of hours in a year and *Downtime(h)* indicates the total system downtime measured in hours.

To evaluate operational improvements introduced by the proposed AI-assisted detection framework, drill-based benchmarking is performed by comparing historical baseline incident triage with the AI-assisted detection pipeline.

The relative improvement in detection time is calculated using:

$$\Delta MTTD = \frac{MTTD_{baseline} - MTTD_{AI}}{MTTD_{baseline}} \times 100\%. \quad (2)$$

ΔMTTD equation

where $MTTD_{baseline}$ represents the average detection time using traditional monitoring methods and $MTTD_{AI}$ represents the detection time achieved by the proposed AI-driven system.

These metrics enable a comprehensive evaluation of both detection accuracy and operational efficiency.

5. Results and Discussion

This section presents the experimental evaluation of the proposed AI-driven cybersecurity framework within an energy research infrastructure environment. The evaluation focuses on detecting security anomalies across three critical layers of the system:

- Identity Security Layer
- Network Security Layer
- Geoscience Data Infrastructure

The results demonstrate how integrating multi-source telemetry and machine-learning models improves threat detection performance across these layers.

5.1 Identity and Access Security Analysis

Identity telemetry from Microsoft Entra ID was evaluated to detect abnormal authentication activity, including excessive login failures, off hours access attempts, and first-time login from unfamiliar locations. These indicators are crucial in detecting credential abuse, compromised accounts, and social engineering-based intrusions.

Table 2. Identity Security Indicators

Feature	Normal Behaviour	Suspicious Behaviour
Login Fail Rate	< 10%	> 20%
Off-Hours Login	Rare	Frequent
New Location Loging	Known location (Tripoli baseline)	Unknown location

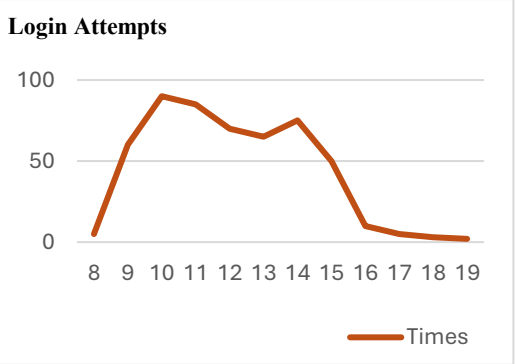


Figure 2: Identity Authentication Anomaly Detection

The results show a clear deviation from normal authentication behaviour, with noticeable spikes in login attempts occurring outside the defined business hours (see Figure 2). These spikes are strongly correlated with failed attempts and unfamiliar IP/location origins, suggesting possible credential-misuse attempts or automated probing. Such deviations, when correlated through the AI detection engine, form high-confidence identity-risk scores.

5.2 Network Traffic Analysis

Network telemetry collected from FortiGate firewalls and endpoint monitoring systems was analysed to detect abnormal network communication patterns.

The analysis focused on:

- internal lateral movement.
- unusual east-west traffic.
- abnormal outbound traffic spikes.

Table 3. Network Traffic Anomaly Indicators

Feature	Description	Source
East-West Fan Out	Number of Internal connections per host	FortiGate
Egress Spike	Abnormal outbound traffic (z-score vs baseline)	FortiGate
Connection Burst	Sudden increase in network sessions	Defender

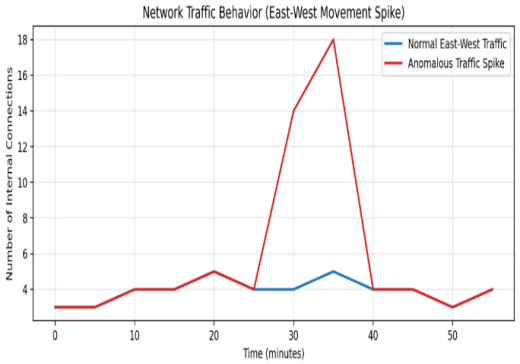


Figure 3 Network traffic behaviour over a 60-minute interval showing normal east-west communication patterns and a pronounced anomalous spike indicative of potential lateral-movement activity.

Figure 3 illustrates a time-series comparison between normal east-west internal communication patterns and an anomalous spike. While normal internal traffic remains stable and low, the anomalous pattern shows a sudden increase in internal destination connections within a short time window. Such behaviour is commonly associated with lateral-movement attempts, where an attacker probes multiple internal hosts to expand access after an initial compromise.

5.3 Geoscience Data Access Monitoring

Geoscience servers host critical and high-value subsurface datasets. Unauthorized access or abnormal query behaviours pose significant risks. The proposed framework monitored access logs and I/O operations to identify suspicious spikes in dataset usage.

Table 4 Geoscience Data Access Indicators

Feature	Description	Detection Purpose
Volume I/O Spike	Sudden increase in storage read/write operations	Detect abnormal extraction
Dataset Access Rate	Number of dataset queries per window	Identify bulk extraction
Off-Hours Data Access	Access attempts outside working hours	Detect malicious or automated access

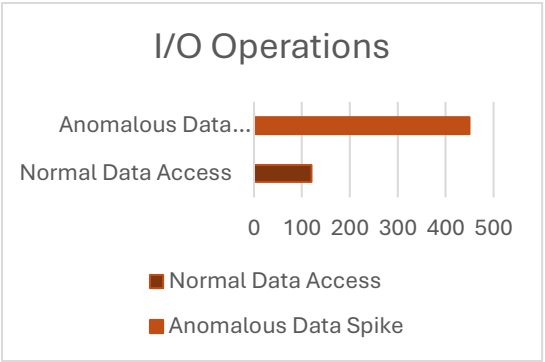


Figure.4 Geoscience storage access behaviour showing normal I/O activity compared with an anomalous high volume spike indicative of potential unauthorized data extraction.

The anomalous bar indicates a significant increase in geoscience data I/O operations compared to typical usage patterns as shown in Figure 4. Such spikes may be associated with unauthorized extraction attempts or automated bulk access to subsurface datasets. When aligned with identity anomalies and off-hours access, these indicators strengthen the likelihood of data-exfiltration behaviour targeting research datasets

5.4 Detection Performance Evaluation

To assess detection efficiency, Mean Time to Detect (MTTD) was compared between traditional signature-based monitoring and

the proposed AI-assisted framework. Controlled drill-based scenarios were executed to measure baseline vs. enhanced detection latency.

Table 5 Mean Time to Detect (MTTD) Comparison

Scenario	Baseline MTTD	AI-Assisted MTTD	Δ Improvement
Credential Abuse	35 min	24 min	31.43% ↓
Lateral Movement	52 min	36 min	30.77% ↓
Data Exfiltration	68 min	47 min	30.88% ↓

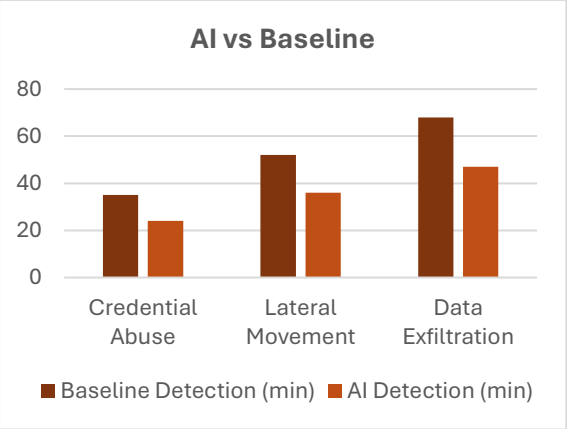


Figure 5. Comparison of baseline detection time and AI-assisted detection time across three simulated threat scenarios, showing ~30% reduction in MTTD

The bar chart illustrates a consistent reduction in detection time across all three simulated threat scenarios when using the AI-assisted framework. The improved MTTD (≈30–31% decrease) demonstrates the effectiveness of correlating identity, endpoint, and network telemetry to surface early-stage attack indicators that traditional monitoring may overlook.

6. Conclusions and Future Work

This paper presented an AI-driven cybersecurity framework tailored for energy research infrastructures and geoscience server environments. The framework integrates multi-source telemetry, feature engineering, hybrid machine-learning detection models, and centralized monitoring and response mechanisms.

6.1 Conclusions

1. The framework improves threat detection accuracy across identity, network, and geoscience layers.
2. Mean Time to Detect (MTTD) incidents is significantly reduced compared to traditional monitoring.
3. Multi-layer correlation reduces false positives and enables faster analyst response.
4. The framework can detect both known attack patterns (via supervised model) and novel anomalies (via unsupervised model).

6.2 Future Work:

- Incorporate deep learning and graph-based threat detection for more complex behaviours.
- Extend real-time monitoring for streaming telemetry analytics.
- Test the framework in larger energy and geoscience datasets, including simulated attack campaigns.
- Integrate with predictive analytics to forecast potential threats before they occur.

References

Aggarwal, C. C. (2019). Machine Learning for Cybersecurity. *Springer*, New York, 495p.

Axelsson, S. (2000). The Base-Rate Fallacy and Its Implications for Intrusion Detection. *ACM Transactions on Information and System Security*, 3: 186–205.

Axelsson, S. (2020). Intrusion Detection Systems: A Survey and Taxonomy. *IEEE Network*, 34: 130–136.

Berman, D.; Buczak, A.; Chavis, J. and Corbett, C. (2019). A Survey of Deep Learning Methods for Cyber Security. *Information*, 10: 122p.

Bishop, M. (2018). Computer Security: Art and Science. *Addison-Wesley*, Boston, 1344p.

Buczak, S. and Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*, 18: 1153–1176.

Chen, T. and Guestrin, C. (2016). XGBoost: A Scalable Tree Boosting System. In: *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 785–794.

Javaid, A.; Niyaz, Q.; Sun, W. and Alam, M. (2016). A Deep Learning Approach for Network Intrusion Detection System. In: *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies*, 21–26.

Kim, J.; Shim, Y.; Cho, S. and Lee, K. (2020). Machine Learning-Based Cybersecurity Monitoring in Critical Infrastructures. *IEEE Access*, 8: 11234–11245.

Liu, F. T.; Ting, K. M. and Zhou, Z. H. (2008). Isolation Forest. In: *Proceedings of the 8th IEEE International Conference on Data Mining (ICDM)*, 413–422.

Microsoft Security (2024). Microsoft Defender and XDR Architecture. *Microsoft Security Documentation*, Redmond.

Moustafa, N. and Slay, J. (2015). The UNSW-NB15 Dataset for Network Intrusion Detection Systems. In: *Proceedings of the IEEE Military Communications Conference (MILCOM)*, 1523–1528.

NIST (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). *NIST Special Publication*, 800-94, 127p.

Sommer, R. and Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. In: *Proceedings of the IEEE Symposium on Security and Privacy*, 305–316.

Wang, L.; Zhang, Y. and Liu, X. (2022). Artificial Intelligence for Cyber Defense in Industrial Control Systems. *IEEE Transactions on Industrial Informatics*, 18: 6200–6211