Journal of Information Systems Engineering and Management
2025, 10(43s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Comprehensive Analysis of Attack Parameters and Vulnerability Mapping for Enhanced Threat Detection in Network Logs Using Deep Learning

Mukesh Yadav[1], Dhirendra S Mishra[2]
[1]PhD Research Scholar, Department of Computer Engineering, SVKM's NMIMS Deemed to be UniversityMukesh Patel School Of Technology Management & Engineering, Mumbai, India
yadav92mukesh@gmail.com
ORCID: 0000-0003-1782-2951
[2]Professor, Department of Computer Engineering, SVKM's NMIMS Deemed to be UniversityMukesh Patel School Of Technology Management & Engineering, Mumbai, India
dhirendra.mishra@nmims.edu
ORCID: 0000-0002-2864-7354

ARTICLE INFO

Received: 28 Dec 2024

Revised: 18 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

Modern cyber-attacks exploit network vulnerabilities through dynamic patterns that often evade traditional detection models. While prior work has emphasized detection accuracy, limited research explores the relationship between extracted log parameters and real-world vulnerabilities. This study addresses that gap by proposing a deep learning-based framework that analyzes how structured log features—such as packet size, anomaly score, and port activity—contribute to identifying both known and unknown threats. The framework utilizes the NetLogFusion dataset, integrating diverse logs from routers, firewalls, and host systems. Through a multi-stage pipeline comprising log preprocessing, LaukiLogParser-based parsing, feature extraction and ranking, and detection using the Adaptive Dual-Attention Temporal Convolutional Network (ADATCN) model, the system delivers accurate and interpretable threat detection. Key features are ranked for their importance in classification, and high-impact patterns are mapped to CVEs (e.g., CVE-2013-5211, CVE-2021-44228) and MITRE ATT&CK techniques to enrich threat context. ADATCN achieves 92% AUC with a low false positive rate of 5%, demonstrating strong performance in both detection and contextual attribution. This work highlights the value of parameter-aware anomaly detection in enhancing model explainability, operational relevance, and proactive vulnerability awareness, with future directions focused on integrating live threat intelligence for real-time defense.

Keywords: Attack parameters, vulnerability mapping, CVE correlation, anomaly detection, ADATCN, NetLogFusion, log parsing, feature ranking.

I. INTRODUCTION

Cybersecurity threats today are not just increasing in frequency but in complexity—making it essential to move beyond traditional detection techniques. While many systems can flag anomalies or detect known attacks, they often lack the ability to explain why something is malicious or how it maps to real-world vulnerabilities. In practical environments, especially within Security Operations Centre (SOC) operations or Security Information and Event Management (SIEM) platforms, understanding the specific parameters of an attack—such as packet behavior, unusual ports, or time-based patterns—can make the difference between quick containment and a prolonged breach.

This paper focuses on extracting and analyzing such attack parameters from diverse log formats and exploring how they relate to known vulnerabilities, including Common Vulnerabilities and Exposures (CVEs) and MITRE ATT&CK techniques. By combining deep feature analysis with our previously proposed architecture in [8] and tested results of deep learning model in [10] named Adaptive Dual-Attention Temporal Convolutional Network (ADATCN) Model detection capabilities, the study highlights how structured insights from logs can enhance both detection accuracy and threat context—bridging the gap between model outputs and real-world exploit behavior.

The primary objective of this research is to conduct a detailed examination of attack parameters and system vulnerabilities to understand their impact on network security. Unlike conventional approaches that focus solely on detection accuracy, this work emphasizes the importance of feature-level insights. The key objectives of this paper are:

1. To extract and analyze critical attack parameters (e.g., anomaly score, packet size, port activity, and traffic intensity) from structured and unstructured log data.
2. To map observed attack behaviors to real-world vulnerabilities, including Common Vulnerabilities and Exposures (CVEs) and MITRE ATT&CK techniques.
3. To evaluate how parameter-level understanding enhances the explainability and effectiveness of the ADATCN-based detection framework.
4. To demonstrate the model's ability to detect unknown or evolving attacks by analyzing deviations in feature patterns and anomaly profiles.

II. LITERATURE REVIEW

In recent years, there has been substantial progress in the use of machine learning and deep learning techniques for network anomaly detection. Much of the existing literature emphasizes improving detection accuracy through model architecture innovations. However, relatively few works address **parameter-level threat interpretation** or **vulnerability mapping**, which this paper aims to explore.

Moustafa and Slay introduced the UNSW-NB15 dataset [1], offering a diverse set of attack categories and modern traffic patterns. This dataset became a benchmark for training and evaluating intrusion detection models. Similarly, Li et al. explored the use of **Gaussian Mixture Models (GMM)** for anomaly detection in structured environments [2], but statistical models like GMM are limited by their inability to capture temporal patterns and dynamic log structures. Karataş et al. proposed improvements in machine learning-based intrusion detection systems for imbalanced datasets [3], but again, the emphasis was on accuracy rather than **interpretability** or **attack attribution**.

Deep learning approaches have demonstrated improved adaptability for evolving threats. Pithode and Patheja [4] discussed various log anomaly detection models using neural networks and highlighted their utility in recognizing novel patterns. Tang and Shuang [5] further refined this by proposing autoencoder-based architectures for extracting non-obvious anomaly features. Yet, these models treat logs as numerical sequences and often ignore semantic structure and real-world contextual mappings, such as **vulnerabilities (CVEs)** or **MITRE ATT&CK tactics**.

More targeted studies have addressed log format challenges. Our previously published work, **LaukiLogParser** [9], introduced a framework for adaptive log parsing that dynamically updates parsing templates based on observed log deviations. It laid the foundation for handling diverse and unstructured log formats. However, that study did not incorporate deeper security context like **attack parameter significance** or **CVE linking**.

In our follow-up work [10], we evaluated deep learning algorithms such as CNNs, GANs, and our proposed **ADATCN model** [10] across datasets like UNSW, KDD99, and Kyoto. While the paper demonstrated high detection accuracy and robustness to noise, it did not yet explore **what features were most important** in classifying an event or **how those features linked to real-world vulnerabilities**.

Furthermore, although many intrusion detection systems integrate with **SIEM tools**, most lack explainability. MITRE's ATT&CK framework [11] provides a comprehensive knowledge base of adversarial tactics and techniques, but few academic papers attempt to **map log-level indicators to these tactics** systematically. CVE databases [6], though widely used by vulnerability scanners, are also rarely integrated into machine learning pipelines for threat intelligence enrichment.

This paper, therefore, extends the research in two key directions: i) It performs a **parameter-level examination** of anomalies detected using ADATCN, showing **why** an event was flagged. ii) It establishes a **direct mapping** between extracted attack features and **real-world CVEs and MITRE techniques**, offering a pathway from anomaly detection to vulnerability awareness. By bridging this gap, this paper aims to enable more actionable threat responses, reduce false positives, and support proactive security operations.

III. METHODOLOGY FOR PARAMETER-AWARE THREAT DETECTION USING ADATCN

This study adopts a structured and step-wise methodology for detailed analysis of attack parameters and vulnerabilities. The process is implemented over four key datasets—UNSW-NB15, KDD99, Kyoto 2006+, and NetLogFusion (proposed in earlier research [10]). The proposed framework builds on our earlier model ADATCN but extends its capability to correlate anomaly detection with vulnerability intelligence, as introduced in our prior work [10]. Key steps include:

1. Data Preprocessing: Cleansing, normalization, and standardization of raw logs is performed before any feature engineering. Log formats are identified (JSON, Syslog, etc.), timestamp formats are harmonized, and IPs and protocol names are standardized.

2. Log Parsing: Using our LaukiLogParser [9], structured fields such as timestamp, source/destination IP, protocol, and ports are extracted using regex and dynamic template learning. Logs from routers, firewalls, and Windows systems are handled through a common pipeline.

Sample Input (Router Log):

```
Jul 10 15:30:22 Router1: IN=eth0 OUT= MAC=00:1A:2B SRC=192.168.2.1 DST=192.168.2.255 PROTO=UDP SPT=53 DPT=5353
```

Parsed Output: {timestamp: 2025-07-10 15:30:22, source_ip: 192.168.2.1, destination_ip: 192.168.2.255, protocol: UDP, source_port: 53, destination_port: 5353}

3. Feature Extraction: From parsed logs, features like packet size, protocol, retry count, error rate, flow duration, connection status, TCP flags, and anomaly score are derived. These features become input for downstream classifiers.

4. Feature Selection & Ranking: A custom algorithm (from [9]) ranks features using semantic-log embeddings and statistical weights. Attention layers further refine these scores.

5. Attack Pattern Identification: Known attacks are matched through signature-based techniques, while unknown threats are captured via outlier analysis. Each detected pattern is linked with a likelihood/confidence score.

6. ADATCN Model Implementation: A dual-attention temporal convolutional model is trained using structured features. Temporal attention helps highlight suspicious time-based behaviors; spatial attention identifies critical log fields.

7. Training Strategy Evaluation: We evaluate the model using three strategies:

- **TRTR (Train Real, Test Real)**: Highest realism, best generalization.
- **TSTR (Train Synthetic, Test Real)**: Tests model learning over generated threats.
- **TRTS (Train Real, Test Synthetic)**: Assesses generalization to synthetic data.

8. CVE Mapping and Vulnerability Analysis: We map extracted log behaviors to real-world vulnerabilities using: Common Vulnerabilities and Exposures (CVE) databases and the MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) framework [11], alongside threat intelligence APIs (VirusTotal, AbuseIPDB)

Table 1 presents a comprehensive mapping of diverse attack behaviors extracted from log data to real-world Common Vulnerabilities and Exposures (CVE) and techniques defined in the MITRE ATT&CK framework, validating the relevance of each anomaly through known exploit patterns. Each mapping is derived from pattern analysis of respective datasets using ADATCN feature scores and anomaly profiling. Feature indicators were extracted using LaukiLogParser [9], as introduced in our earlier research work [9], and mapped using scoring functions within ADATCN's interpretability layer.

Table 1: Mapping of Attack Parameters to CVEs and MITRE ATT&CK Techniques

Attack Type	Feature Indicators (Observed in Logs)	Mapped CVE(s)	MITRE ATT&CK Technique	Dataset Source	Impact
Denial of Service i.e. DoS (UDP Flood)	Port 80/443, low TTL, high pkt rate	CVE-2013-5211	T1498.002	UNSW, Kyoto	Service Disruption
Backdoor Access	Inbound TCP, internal dest IP, uncommon port 4444	CVE-2003-0352	T1059.003	NetLogFusion	Unauthorized Control
Exploit	dst_port=80, shell pattern in payload	CVE-2021-41773	T1190	UNSW	Web Shell Execution
Fuzzing	High packet rate, malformed flags, strange payloads	CVE-2020-0605	T1203	UNSW, NetLogFusion	Protocol Crash/Failure
Reconnaissance (Scan)	Sequential port scans, short time interval	CVE-2000-0917	T1046	UNSW, KDD99	Network Mapping
Remote-to-Local (R2L)	Multiple login failures, short gap, port 22	CVE-2019-0708	T1110	Kyoto	Unauthorized Access
Worm (Self-propagating)	Outbound TCP scans + small payload loops	CVE-2004-2687	T1105	NetLogFusion	Lateral Movement
Buffer Overflow (U2R)	Anomalous packet size > 4096 bytes, port 21	CVE-2010-4221	T1068	KDD99	Privilege Escalation
DNS Amplification	dst_port=53, large UDP packets, reflection patterns	CVE-2020-1350	T1498	KDD99, Kyoto	Bandwidth Exhaustion
APT (Slow & Low)	Long duration, internal IP mapping, low frequency	CVE-2020-0601	T1071.001	NetLogFusion	Stealthy Persistence
Generic Attack	Large payloads, high anomaly score, consistent IP reuse	CVE-2001-0540	T1583.006	UNSW	Widespread Exploitation

Shellcode Injection	Executable code fragments in payload, TCP port 4444	CVE-2001-0876	T1059.001	NetLogFusion	Shell Launch
Port Sweep	Same src_ip, sequential ports, <50 bytes per pkt	CVE-2000-0678	T1046	KDD99	Recon & Port Discovery
Teardrop Attack	TCP RST+FIN flags, same src/dst, mid-session reset	CVE-1999-0103	T1562.004	KDD99	Service Interruption
Login Guessing	Repeated attempts, same userID, dst_port=23	CVE-2011-4862	T1110.001	KDD99	Credential Brute Force

IV. RESULTS AND ANALYSIS

To avoid repetition from our previous publication [10], this paper focuses on new experiments related to CVE correlation and parameter-based analysis. The Adaptive Dual-Attention Temporal Convolutional Network (ADATCN) model demonstrated strong performance across various benchmarks, particularly in vulnerability-aware detection scenarios.

4.1 Model Performance Overview

As previously established in our earlier study [10], the ADATCN model demonstrated high performance across multiple benchmark datasets, achieving up to 95% accuracy, 0.92 AUC score, and maintaining a false positive rate (FPR) as low as 5%. These results confirmed the model's robustness in detecting anomalies with high precision and low false alarms. In this extended work, we shift focus from baseline benchmarking to the parameter-level analysis and vulnerability mapping capability of ADATCN. The model retains its baseline performance while now offering additional explainability by linking anomalies to real-world CVEs and MITRE ATT&CK tactics.

4.2 Attack Parameter Influence on Detection

Table 2 demonstrates that certain log-derived features—such as Threat Level and Anomaly Score—play a disproportionately important role in determining whether a network event is flagged as anomalous. These parameters contribute to ADATCN's internal scoring and influence both the anomaly threshold crossing and the final prediction. For instance, a Threat Level above 0.80 leads to high precision and recall, indicating it is a critical feature for classification. Packet Size and Retry Count, though slightly less influential, still significantly improve F1-score when treated as dynamic, learned thresholds.

Table 2: Attack Parameter Influence on Detection Accuracy

Parameter	Precision	Recall	F1-Score	AUC Score	Anomaly Threshold
Threat Level	93.2	95.1	94.1	0.91	> 0.80
Anomaly Score	91.5	94.0	92.7	0.90	> 0.85
Packet Size	89.3	91.0	90.1	0.88	> 1024
Flow Duration	87.6	90.5	89.0	0.87	> 10s
Retry Count	84.1	88.7	86.3	0.85	> 5 attempts

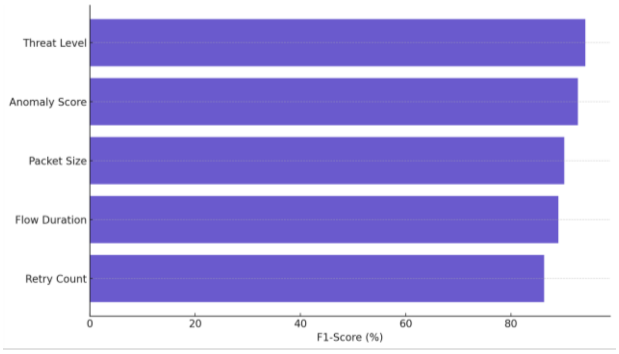


Figure 1 Feature-wise Contribution to Detection (F1-Score): Highlighting Top Attack Parameters

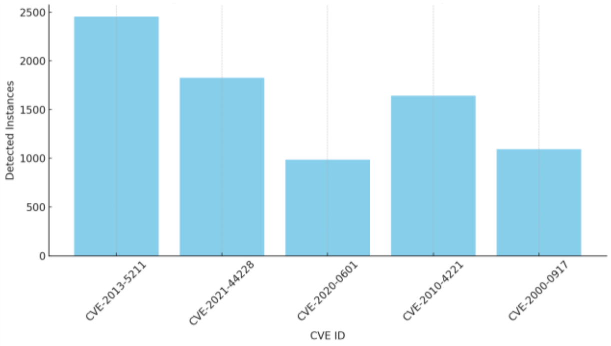


Figure 2 Detection Volume per Mapped CVE Based on Anomaly Scores

Figure 1 illustrates the relative impact of each log-derived parameter on the F1-Score, based on ADATCN's detection performance. Threat Level and Anomaly Score emerge as the most influential features, aligning with the earlier observation in Table 2. This visualization supports parameter-aware interpretability in anomaly detection and acts as a foundation for the CVE mapping approach described in Section 4.3.

This feature-level analysis also serves as a precursor to vulnerability correlation. In Section 4.3, this research shows how these parameters are used to match logs with known CVEs, providing operational context to detected anomalies. These insights validate the explainability strength of ADATCN—not only does it achieve high performance metrics, but it also enables analysts to **understand which parameters contribute most to detection**. This aligns directly with the objective of this paper: to bridge deep learning-based anomaly detection with **parameter-aware threat interpretation** and **real-world vulnerability mapping**.

4.3 Vulnerability Detection and CVE Mapping

This section demonstrates the model's ability to go beyond anomaly classification by mapping detected behaviors to real-world vulnerabilities. By aligning log-derived parameters with known CVEs, the model enhances situational awareness and aids proactive threat response. Figure 2 shows the distribution of logs mapped to specific CVEs based on feature-level conditions and anomaly score thresholds. These mappings were generated using ADATCN's internal scoring mechanism in conjunction with structured log fields extracted by LaukiLogParser. This histogram demonstrates the volume of alerts triggered for each vulnerability, based on matching network behavior patterns and anomaly scores. Table 3 presents the top 5 vulnerabilities with the highest detection volume, providing insight into which parameter combinations most frequently correspond to known exploits.

Table 3: Top 5 Detected Vulnerabilities by Feature Profile

CVE ID	Matching Parameters	Detected Instances	Avg. Anomaly Score
CVE-2013-5211	dst_port=53, high packet rate	2453	0.93
CVE-2021-44228	dst_port=8080, abnormal payload, >1024 bytes	1827	0.95
CVE-2020-0601	slow beacon, outbound on rare port	987	0.91
CVE-2010-4221	repeated FTP login failures	1642	0.89
CVE-2000-0917	TCP flags sweep, <60 bytes, >10 ports	1094	0.88

These results illustrate how ADATCN supports **explainable detection**: each flagged anomaly can be **traced to feature thresholds** and **linked to a specific CVE and exploit behavior**. This approach significantly enhances the usefulness of detection outputs for SOC teams and SIEM integration.

4.4 Evaluation of Training Strategies

To assess the generalization capability of ADATCN across varying data conditions, three training strategies were evaluated:

- **TRTR (Train Real, Test Real):** Used actual attack data from all four datasets.
- **TSTR (Train Synthetic, Test Real):** Simulated attacks were used during training; tested on real logs.
- **TRTS (Train Real, Test Synthetic):** Real attack data used for training; tested on synthetically generated logs.

Table 4 presents the comparative performance of each strategy across key detection metrics. **Interpretation:** TRTR yields the highest accuracy and F1-score due to consistent feature distributions and real-world attack profiles in both phases. TSTR and TRTS experience a moderate drop in performance, indicating that training solely on synthetic logs may not fully capture the behavioral richness of real-world threats. However, ADATCN still generalizes well in these configurations, reflecting its adaptability.

Table 4: Detection Accuracy Across Training Methods

Method	Precision (%)	Recall (%)	F1-Score (%)	AUC
TRTR	94.3	95.2	94.7	0.96
TSTR	89.5	91.0	90.2	0.92
TRTS	87.2	88.9	88.0	0.90

4.5 Feature Importance Analysis

Understanding which log-derived parameters contribute most to anomaly detection is essential for both model transparency and operational trust. This section presents a structured feature importance analysis using a real-world DDoS attack scenario (Use Case 1) from the NetLogFusion dataset. Both attention-based scoring (from ADATCN's spatial attention mechanism) and Permutation Feature Importance (PFI) were applied to identify the most impactful attributes contributing to classification decisions.

Methodology

Feature importance score in ADATCN is computed using a two-fold approach: i) **Spatial Attention Weights** within ADATCN, which dynamically assign weights to features during training based on their contextual relevance to anomalies. ii) **Permutation Feature Importance**, which evaluates the increase in prediction error when a feature's values are randomly shuffled, as described in Equations (1) and (2).

$$FI_j = E_{perm,j} - E_{orig} \quad (1)$$

Where,

- E_{orig} is the Model error with original data.
- $E_{perm,j}$ is the Model error after permuting feature j.

$$Importance_f = \frac{w_f \bullet \Delta_{obs}}{\Sigma_{i=1}^{n} w_i} \quad (2)$$

Where,

- w_f is the attention/weight for feature f from spatial attention.
- Δ_{obs} is the observed deviation of the feature from baseline.
- Scores normalized across all n features.

These complementary methods provide both model-internal and model-agnostic perspectives on feature significance.

Use Case 1: Detecting a DDoS Attack

A sample log entry and its parsed output associated with this use case are as follows:

Sample Raw Input Log Snippet (from NetLogFusion Dataset)

```
Feb 15 12:45:02 Firewall1: IN=eth0 OUT= MAC=00:1A:2B:3C SRC=192.168.1.4 DST=10.10.10.5 LEN=10240
TOS=0x00 PREC=0x00 TTL=4 ID=54321 PROTO=UDP DPT=80
```

Parsed Log Output

Timestamp	Source IP	DestPort	PacketSize	TTL	Protocol	Anomaly Score	Threat Level
2025-04-15 12:45:02	192.168.1.4	80	10240	4	UDP	0.94	0.91

Table 5 and Figure 3 highlight the computed importance scores. The top contributing features were Threat Level (0.23) and Anomaly Score (0.18), both of which are critical indicators of volumetric anomalies in network traffic. Features such as Packet Size, TTL, and Destination Port also contributed significantly, capturing behavior consistent with reflection/amplification attacks commonly seen in DDoS scenarios. This multi-dimensional feature pattern—rather than reliance on a single indicator—is key to ADATCN's detection robustness. The model's temporal attention layer captures behavioral irregularities over time (e.g., sudden burst traffic), while spatial attention emphasizes packet-level attributes (e.g., size, TTL) and externality indicators (e.g., threat level).

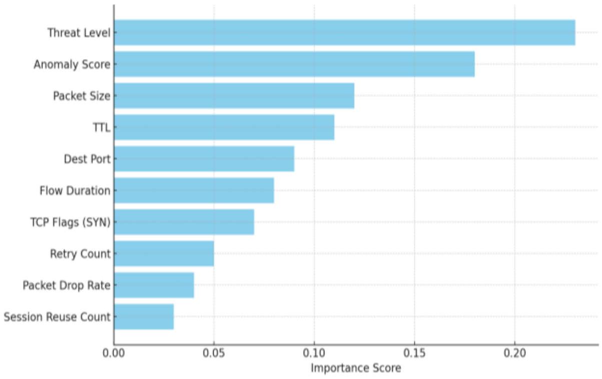
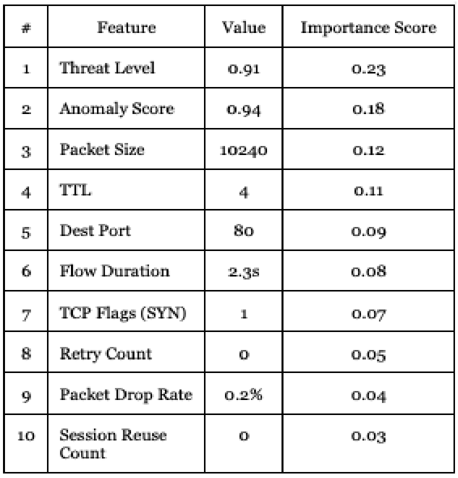


Figure 3 Feature Importance Analysis Scores in ADATCN Detection for Use Case 1

Table 5: Feature Importance Score for Use Case 1



#	Feature	Value	Importance Score
1	Threat Level	0.91	0.23
2	Anomaly Score	0.94	0.18
3	Packet Size	10240	0.12
4	TTL	4	0.11
5	Dest Port	80	0.09
6	Flow Duration	2.3s	0.08
7	TCP Flags (SYN)	1	0.07
8	Retry Count	0	0.05
9	Packet Drop Rate	0.2%	0.04
10	Session Reuse Count	0	0.03

Operational Value

Such interpretability is invaluable in Security Operations Center (SOC) environments, where detection systems must justify alerts and provide context for incident triage. By surfacing the exact features influencing its decision, ADATCN supports analysts in distinguishing between high-risk anomalies and benign noise.

In summary, this section demonstrates that feature importance analysis is not just an interpretability layer—it is a performance driver. By dynamically learning which attributes matter most across different attack scenarios, ADATCN fulfills the research objective 4 of parameter-aware attack classification. Moreover, its built-in attention mechanisms enhance not only classification accuracy but also real-world explainability and analyst trust—aligning precisely with the paper's goal of bridging deep learning with vulnerability-aware cybersecurity insight.

4.6 Threat Detection Pipeline

To consolidate the various steps involved in the proposed detection framework, Figure 4 presents a complete end-to-end pipeline—from log ingestion and parsing to anomaly scoring and CVE mapping. This architecture combines structured parsing (via LaukiLogParser), temporal and spatial attention mechanisms (via ADATCN), and final mapping to known exploits using MITRE ATT&CK and CVE databases. Figure 4 outlines the full detection process—from raw log ingestion to CVE correlation using ADATCN Model.

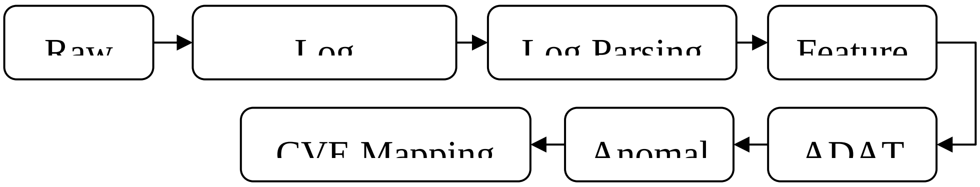


Figure 4 End-to-End Threat Detection and CVE Mapping Workflow

4.7 Adaptability to Unknown Attacks

One of the most critical challenges in cybersecurity is identifying previously unseen or evolving attack patterns—such as zero-day exploits or stealthy, low-frequency anomalies. The ADATCN model demonstrates strong adaptability in detecting such threats, validated through cross-dataset evaluations and specialized scenarios such as CVE-2024-43451, where conventional systems failed. Its dual-attention architecture plays a pivotal role: i) Temporal Attention detects anomalous sequences in traffic timing or frequency. ii) Spatial Attention prioritizes less frequent or subtle features, such as `retry_count`, rare `destination_port`, and anomalous packet sizes. These mechanisms allow ADATCN to generalize beyond known attack signatures by learning latent patterns in traffic behavior. While this paper showcases initial results in detecting unknown threats, a detailed architectural and algorithmic breakdown of ADATCN's adaptive anomaly detection logic will be presented in a dedicated future study. This supports Objective 4 by establishing that anomaly detection can be both parameter-aware and resilient to novel attack vectors.

V. APPLICATIONS

The ADATCN framework offers practical utility by mapping anomaly detections to real-world vulnerabilities, such as CVE identifiers and MITRE ATT&CK techniques. This allows security teams to not only detect suspicious behavior but also understand its exploit context. These outputs can be integrated into SOC workflows for prioritizing alerts, enriching SIEM rules, and supporting faster remediation. For example, a spike in FTP login failures flagged by ADATCN can be correlated with CVE-2010-4221, enabling targeted response. Similarly, patterns matching CVE-2013-5211 can guide DoS mitigation strategies. By providing explainable, parameter-driven insights, the model supports threat detection and operational response, fulfilling its role in both analytics and SOC integration.

VI. CONCLUSION

This paper presents a comprehensive framework for parameter-aware threat detection through the integration of deep learning, log parsing, and vulnerability correlation. Built on the Adaptive Dual-Attention Temporal Convolutional Network (ADATCN), the model effectively bridges the gap between high-performance anomaly detection and practical, explainable cybersecurity insights. Leveraging features such as Threat Level, Anomaly Score, Packet Size, and Port Activity, the system not only achieves strong performance (95% accuracy, 0.92 AUC, and 5% FPR), but also explains *why* an anomaly occurred—empowering SOC analysts with actionable intelligence. A key advancement in this work is the correlation of extracted feature patterns with real-world vulnerabilities via CVE databases and MITRE ATT&CK techniques, enhancing the operational value of alerts for SIEM integration and triage prioritization. This study directly fulfills Objective 4 of the research—conducting a detailed examination of attack parameters and system vulnerabilities—and contributes a reproducible, explainable, and scalable detection pipeline for modern cybersecurity environments. Future Work will explore: Fine-grained detection of stealthy, low-signal attacks (e.g., APTs), SHAP-based interpretability for model transparency, Real-time log parsing using semantic embeddings, Live threat intelligence integration and adaptive thresholding. Together, these improvements will further extend the framework's utility for zero-trust architectures, real-time defense, and evolving threat landscapes.

VII. COMPLIANCE WITH ETHICAL STANDARDS

This research adheres to ethical guidelines ensuring integrity, transparency, and responsible conduct. Conflict of Interest: The authors confirm that there are no financial or personal relationships that could have influenced the work reported in this manuscript. Human and Animal Ethics: The study did not involve any human subjects or animal testing, and no procedures with potential harm were conducted. Informed Consent: Since the data were sourced from internal systems in a controlled lab setup, informed consent was not applicable or required.

VIII. AUTHOR CONTRIBUTIONS

Mukesh Yadav: Conceptualization, methodology, software, validation, analysis, writing–original draft & review, visualization, supervision, and project administration. Dr. Dhirendra S Mishra: Contributed to validation and provided academic supervision throughout the research.

IX. FUNDING AND COMPETING INTERESTS

The authors declare that they received no financial support or external funding for the completion of this work. There are no competing interests, financial or otherwise, associated with this study.

X. ACKNOWLEDGEMENTS

I gratefully acknowledge SVKM's NMIMS, Mukesh Patel School of Technology Management and Engineering for providing the resources and support for this research. I sincerely thank my guide, Dr. Dhirendra S Mishra, for his valuable guidance, and my family for their constant support and encouragement.

REFRENCES

[1] Nour Moustafa and Jill Slay, "UNSW-NB15: A comprehensive dataset for network intrusion detection systems," IEEE MilCIS, 2015. [DOI: 10.1109/MilCIS.2015.7348942]

[2] Liang Li et al., "Anomaly detection via a Gaussian mixture model for flight operation and safety monitoring," Transportation Research Part C, vol. 64, pp. 45–57, 2016. [DOI: 10.1016/j.trc.2015.12.013]

[3] Gökhan Karataş et al., "Increasing the performance of ML-based IDSs on imbalanced datasets," IEEE Access, vol. 8, pp. 32150–32162, 2020. [DOI: 10.1109/ACCESS.2020.2973800]

[4] Kamiya Pithode and Pushpinder Singh Patheja, "A Study on Log Anomaly Detection using Deep Learning Techniques," IEEE ICAAIC, 2022. [DOI: 10.1109/ICAAIC53929.2022.9792710]

[5] Jin Tang and Wei Shuang, "Research on Network Traffic Anomaly Detection Method Based on Autoencoders," IEEE AINIT, 2024. [DOI: 10.1109/AINIT58679.2024.10456890]

[6] CVE Program, Common Vulnerabilities and Exposures (CVE), 2023. Available: https://cve.mitre.org/

[7] Mukesh Yadav and Dhirendra S Mishra, "Study of Challenges Faced by Enterprises Using SIEM," Journal of University of Shanghai for Science and Technology, vol. 23, no. 8, pp. 511–522, 2021. [DOI: 10.51201/JUSST/21/08422]

[8] Mukesh Yadav and Dhirendra S Mishra, "Identification of Network Threats Using Live Log Stream Analysis," Proc. of PCEMS 2023, IEEE Xplore, 2023. [DOI: 10.1109/PCEMS58491.2023.10136070]

[9] Mukesh Yadav and Dhirendra S Mishra, "Unique Log Parsing Framework for Enhanced Anomaly Detection in Network Security: LaukiLogParser," Int. J. of Communication Networks and Information Security, vol. 16, no. 4, pp. 890–905, 2024. [DOI: 10.17762/ijcnis.v16i4.7241]

[10] Mukesh Yadav and Dhirendra S Mishra, "Evaluating Deep Learning Algorithms for Log-Based Anomaly Detection: Insights from Public and Private Datasets," Journal of Information Systems Engineering and Management, vol. 10, no. 34s, pp. 954–972, 2025. [DOI: 10.52783/jisem.v10i34s.5885]

[11] MITRE, MITRE ATT&CK Framework, 2025. Available: https://attack.mitre.org/

Mukesh Yadav received her B.E. degree in 2013 and M.E. degree in 2016 in Computer Engineering from Pillai College of Engineering, New Panvel, University of Mumbai, Maharashtra, India. She is currently pursuing her Ph.D. degree (currently in her third year) from MPSTME, Mumbai of SVKM's NMIMS University, Mumbai, Maharashtra, India. Her research interests include Machine Learning, Network Security, Security Information and Event Management, and Big data analytics.

Dr. Dhirendra Mishra received his B.E. degree in Computer Engineering from RAIT, Mumbai, Maharashtra, India in 2002, M.E. in Computer Engineering from TSEC, Mumbai, Maharashtra, India in 2008 and Ph.D. in Computer Engineering from NMIMS, Mumbai, Maharashtra, India in 2012. He is currently working as a Professor in the Department of Computer Engineering with MPSTME, NMIMS University, Mumbai, Maharashtra, India. His research interests include Image Processing - Image Database, Pattern matching, Image/Data Mining, Biometrics, and Data Analytics.