AI-Enabled Threat Log Analyzer

An AI-powered solution for cyber threat detection from webserver logs.

Names of the Presenter:

Ansh Aryan (BTECH/10301/22)

Gourab Mahato (BTECH/10317/22)

Abhinav Kumar (BTECH/10318/22)

Name of the Project Supervisor:

Dr. Sitanshu Shekhar Sahu

Department of ECE, BIT,
Mesra, Ranchi-835215

Table of
CONTENTS

Introduction & Motivation

What are logs?

- Logs are machine-generated text or alphanumeric records that capture events and activities of a system or application.

Introduction:

- Cybersecurity today faces a relentless and evolving threat landscape.
- Enterprises today must defend against a wide variety of attacks—adversarial threats, credential misuse, lateral movement, and APTs—often hidden in vast volumes of webserver logs.
- Traditional log analysis techniques (rule-based, template-matching) struggle with high false positives, lack of context, and an inability to detect novel or stealthy attacks.

Motivation: There is a pressing need for AI-powered, semantics-aware log analytics that can surface true threats, provide actionable context, and support explainable, robust decision-making in BFSI and similar sectors.

Objective & Problem Statement

Objective: To design an AI-driven system that detects and predicts anomalies in **Web Server Logs,** by combining feature-engineered and transformer-based methods. A robust, explainable log anomaly detection pipeline, capable of detecting diverse cyber threats from web server logs.

Problem Statement:

How can we move from keyword- or rule-based detection in web logs to a semantics-aware, feature-rich, and explainable detection framework that uncovers hidden attack patterns like reconnaissance, brute force, injection, or privilege abuse.

Literature Review

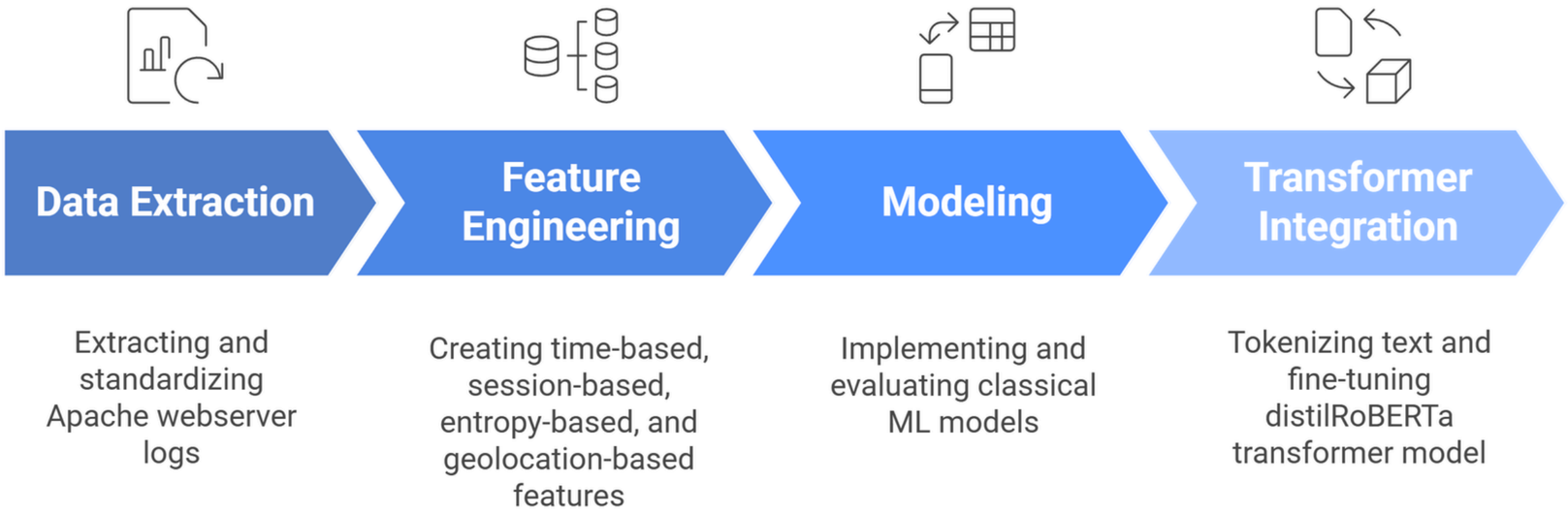
- Many works (e.g., ConceptUML, Electra, GNN-based detectors) excel at anomaly detection, but struggle with explainability, threat mapping, or adversarial robustness.
- Few pipelines support mapping detected anomalies directly to threat knowledge bases (MITRE ATT&CK®, CAPEC™, CWE™) for actionable response.
- There is a lack of solutions that blend semantic embeddings, unsupervised concept learning, explainability, and alert system & co-pilot in one integrated workflow.

S.N.	Paper / Year	Methodology	Main Results	Limitations / Notes
1	LogELECTRA (2024)	ELECTRA token anomaly, self-supervised	F1 ≈ 0.96, parser-free, robust to format changes	Ignores windowed context, no direct threat mapping, point anomaly only
2	LLM4Sec	Fine-tuned LLM sequence classification	Outperforms SOTA log analysis across datasets	Needs labeled logs, interpretability varies, requires high computational resources
3	Interactive Group-Based Log Exploration (2022)	Visual event grouping, analyst-in-loop	Enables interactive grouping, process insights	Limited automated detection, best for exploratory human workflows
4	Threat Log Analyzer (2025, this work)	Did anomaly focused feature eng and transformer methods	DistilRoBERTa ~ 82% Accuracy, DQ= 0.872, DE = 0.128	Provides interpretable anomaly detection, but currently limited by dataset diversity, and adaptive learning.

Proposed Solution

- An AI-powered web log threat analyzer built on Apache log, time-, session-, and entropy-based features, and GeoIP-driven anomaly detection.
- It leverages DistilRoBERTa for semantic classification of log patterns and employs a hybrid interpretability layer using statistical correlation and SHAP analysis.

Flow Graph



Methodology

01. Data Extraction:

- Extracted Apache access/error logs.
- Standardised fields: [**timestamp, IP, request, status, bytes, user agent, referrer**].

02. Feature Engineering:

- Time-based: request rates, inter-arrival times, hourly density.
- Session-based: session length, repeated IP counts, abnormal URI patterns.
- Entropy-based: URL/query entropy, user-agent diversity, byte size variance.
- Geolocation-based: mapping IPs to countries; anomaly detection by region frequency.

03. Modeling:

- Implemented classical ML models (Logistic Regression, Random Forest, Isolation Forest).
- Evaluated feature significance via correlation and SHAP.
- Identified most relevant features for anomaly prediction.

05. Transformer Integration:

- Tokenized preprocessed log text
- Fine-tuned distilroberta-base for binary classification
- Achieved ~82% accuracy on Apache web log dataset

DataSet

src: Apache Access HTTPS server

	ip	datetime	gmt	request	status	size	referer	browser	country	detected	label
8389	182.0.164.207	23-Jul 2019 13:06:12	+0700]	GET /bkd_baru/assets/images/scan_kinerja/.D018...	404.0	1130	http://universitas.com/bkd_baru/hasil_penilaia...	Mozilla/5.0 (Linux; Android 9; SM-A505F) Apple...	Indonesia	AMAN	Normal
33149	64.233.173.166	25-Jul 2019 18:58:41	+0700]	GET /bkd_baru//kinerja_dosen/beri_nilai/8472/D...	200.0	20920	http://universitas.com/bkd_baru/kinerja_dosen/...	Mozilla/5.0 (Linux; Android 8.0.0; SM-J400F Bu...	United States	DICURIGAI	Anomalous
30484	180.178.99.174	25-Jul 2019 9:39:04	+0700]	GET /bkd_baru/assets/images/scan_kinerja/D0188...	206.0	1333	http://universitas.com/bkd_baru/kinerja_dosen/...	Mozilla/5.0 (Windows NT 6.1; rv:50.0) Gecko/20...	Indonesia	AMAN	Normal
130	64.233.173.166	17-Jul 2019 21:22:19	+0700]	GET /bkd_baru/assets/images/scan_kinerja/D0001...	200.0	11832	http://universitas.com/bkd_baru/bidang_pendidi...	Mozilla/5.0 (Linux; Android 9; SM-J400F) Apple...	United States	BAHAYA	Anomalous
7131	180.178.99.174	23-Jul 2019 12:03:40	+0700]	GET /bkd_baru/bidang_pengabdian/edit/OTE4MQ HT...	200.0	26467	http://universitas.com/bkd_baru/bidang_pengabdian	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.3...	Indonesia	AMAN	Normal

- **ip**: The IP address of the client initiating the request (e.g., 114.125.221.132). Repeated IPs may indicate automated or suspicious activity.
- **request**: The specific HTTP request method and resource path.
- **status**: The HTTP response status code returned by the server (e.g., 200 for success, 404 for missing page).
- **size**: The size of the response in bytes, which helps identify abnormal payload sizes or repetitive requests
- **The detection label**: BAHAYA/DICURIGAI for malicious/anomalous requests, and AMAN (“Safe”) for normal traffic.
- **Total DataSet: 37694**
- **We Used: 2000** balanced dataset for training model.
    - 1000 Normal
    - 1000 Anomalous

Results and Discussion

The final GRU model demonstrated exceptional performance, achieving near-perfect classification scores.

Model	Accuracy	F1-Score (Anomalous)	Detection Quality (DQ)	Detection Error (DE)
Logistic Regression	62%	0.13	0.674	0.456
Random Forest	69%	0.41	0.701	0.389
Isolation Forest	77%	0.58	0.742	0.312
DistilRoBERTa	82%	0.81	0.872	0.128

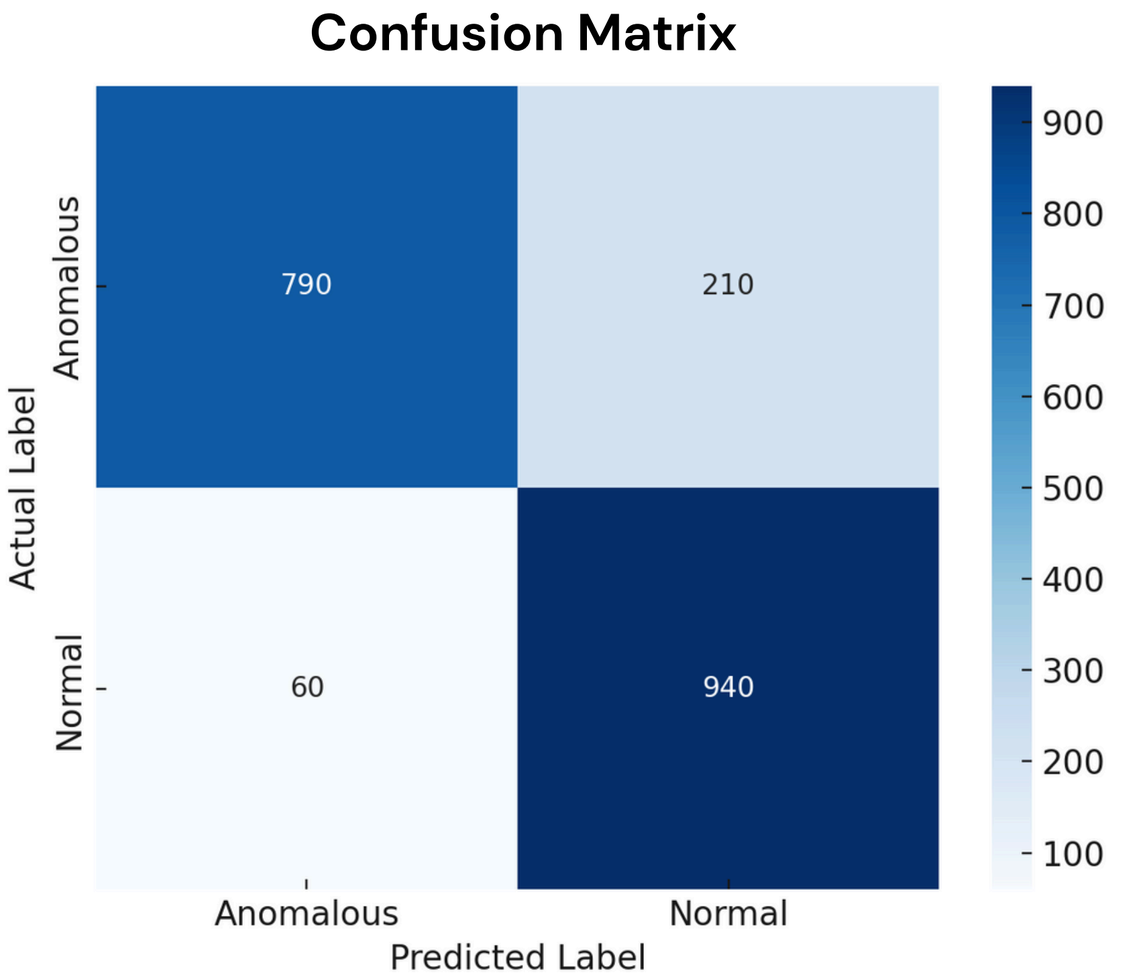
Results & Discussion

DistilRoBERTa vs Classical ML:

- Logistic Regression: 62% accuracy
- Random Forest: 69% accuracy
- Isolation Forest : 77% accuracy
- DistilRoBERTa: 82% overall accuracy, F1=0.81

Model Behavior: DistilRoBERTa captures sequence semantics like attack probes or recon attempts.

Feature Insights: Top anomaly indicators—unusual IP repetition, URL entropy spikes, inconsistent time deltas.



Conclusion

This project establishes the foundation for a web server log-based threat detection framework that merges statistical, semantic, and geographical analysis. DistilRoBERTa demonstrates promising accuracy, validating the approach's potential for production-level expansion.

Future work:

- Extend datasets to Nginx & hybrid web infrastructure.
- Detection of type of anomaly.
- Implement GRU- a lightweight sequential model for context-aware detection.
- Integrate real-time streaming and visualization dashboard (ELK + Flask/React).
- Continue mapping detected anomalies to existing knowledge bases like MITRE ATT&CK®, CAPEC, CWE for actionable insights for SOCs.

References

[1] J. Wu, S. Zhang, H. Liu, and W. Yang, “AAR-Log: a robust log anomaly detection method resisting adversarial attacks,” Computer Networks, vol. 269, pp. 1–15, 2025.

[2] E. Karlsen, X. Luo, N. Zincir-Heywood, and M. Heywood, “Benchmark ing large language models for log analysis, security, and interpretation,” Journal of Network and Systems Management, vol. 32, no. 3, pp. 1–26, 2024.

[3] Y. Yamanaka, T. Takahashi, T. Minami, and Y. Nakajima, “LogELEC TRA: self-supervised anomaly detection for unstructured logs,” in Proc. AAAI Conf. Artificial Intelligence, 2024, pp. 1–8.

[4] X. Han, T. Pasquier, A. Bates, J. Mickens, and M. Seltzer, “UNICORN: runtime provenance-based detector for advanced persistent threats,” in Proc. Network and Distributed Systems Security Symposium (NDSS), San Diego, CA, USA, Feb. 2020, pp. 1–14.

[5] T. Fehrer, L. Moder, and M. R¨oglinger, “An interactive approach for group-based event log exploration,” Information Systems, vol. 134, p. 102575, Jun. 2025.

THANK YOU!

Open to Questions & Suggestions.