Indonesian Journal of Electronics, Electromedical Engineering, and Medical Informatics e-ISSN: 2656-8624
Homepage: https://ijeeemi.org/; Vol. 7, No. 4, pp. 713-723, November 2025

RESEARCH PAPER

OPEN ACCES

Implementation of BERT and RoBERTa Models in Classification Cyberattacks and Anomalies on Web Servers

Edi Dwi Prasetyo[1], Basuki Rahmat[2], and Anggraini Puspita Sari[3]

Master of Information Technology, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Surabaya, Indonesia

Abstract

Cybersecurity is a crucial aspect in maintaining the integrity and availability of information systems, especially on web servers, which are vulnerable to various types of attacks and anomalies. This research aims to investigate the application of transfer learning in classifying cyber attacks and anomalies on web servers. Transfer learning, a powerful approach in deep learning, enables pre-trained models to adapt to new tasks with limited data, offering an efficient solution for detecting malicious activities and unusual patterns in web server logs. The goal is to improve detection accuracy while reducing the time and resources required to train models from scratch. This study employs a bi-layer classification approach utilizing pre-trained Transformer models, specifically BERT and RoBERTa, through transfer learning to detect cyber attacks and anomalies in web server log data. The process includes preprocessing the log data, extracting relevant features, and fine-tuning BERT to classify known attacks in the first layer, followed by RoBERTa in the second layer to detect unusual or unknown behaviors. Model performance is evaluated using accuracy, precision, recall, and F1-score, and the results are compared with traditional deep learning methods, such as BERT and RoBERTa, to highlight the advantages of this bi-layer transfer learning approach. The proposed bi-layer method achieved an accuracy of 0.93, precision of 0.94, recall of 0.92, and F1-score of 0.93, outperforming single-model baselines such as BERT (accuracy 0.85) and RoBERTa (accuracy 0.91). The error rate of the proposed method was approximately 7%, indicating a significant reduction in misclassification compared to BERT (15%) and RoBERTa (9%). The result of this proposed bi-layer classification method is improved performance in detecting cyber attacks and anomalies compared to using BERT and RoBERTa individually. By combining both models, the system is expected to achieve higher accuracy, better precision in identifying true threats, improved recall for detecting a wider range of attacks, and a more balanced F1 score. In conclusion, the proposed bi-layer classification framework demonstrates that combining pre-trained Transformer models through transfer learning can significantly enhance the effectiveness of intrusion detection systems. This approach not only improves detection performance but also ensures scalability and adaptability, making it a viable solution for modern web server security challenges.

Paper History

Received July 17, 2025
Revised October 10, 2025
Accepted October 30, 2025
Published November 10, 2025

Keywords

Cyberattack;
Network anomaly;
BERT;
RoBERTa
Transfer Learning.

Author Email

23066020017
@student.upnjatim.ac.id
basukirahmat.if
@upnjatim.ac.id
anggraini.puspita.if
@upnjatim.ac.id

I. Introduction

In recent years, the rapid growth of the internet has significantly increased the volume and complexity of cyber attacks targeting web servers. These attacks can severely compromise the security and reliability of web services, resulting in data breaches, operational disruptions, and financial losses [1][2][3][4]. As cyber threats become more advanced and evasive, traditional forensic analysis and rule-based detection techniques are increasingly inadequate in detecting and mitigating such threats in real-time [5][6][7].

This research investigates the implementation of transfer learning through a bi-layer classification architecture, utilizing BERT and RoBERTa models for detecting cyber attacks and anomalies in web server environments. Transfer learning, a pivotal technique within the deep learning paradigm, facilitates the adaptation of large-scale pre-trained language models to specific downstream tasks, even when data availability and computational resources are constrained [8][9][10][11]. In this context, the study aims to develop a two-stage classification system that minimizes training overhead while enhancing the accuracy and generalizability of cyberthreat detection. This approach is particularly relevant for dynamic web server environments where rapid detection of diverse and evolving threats is essential.

The design of the classification system begins with BERT in the first layer, serving as the foundational model due to its proven performance in numerous natural language processing (NLP) tasks. As the pioneering model in bidirectional Transformer architectures, BERT

Corresponding author: Edi Dwi Prasetyo, 23066020017@student.upnjatim.ac.id, Master of Information Technology, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.119

establishes a robust baseline for classification by capturing contextual dependencies in sequential log data. Its widespread adoption and demonstrated effectiveness in text classification tasks make it an ideal candidate for benchmarking in the cybersecurity domain. By first applying BERT, researchers are able to evaluate the fundamental capabilities of Transformer-based models in handling structured server log data, while laying the groundwork for more advanced refinements in subsequent layers [12][13].

Building on the baseline established by BERT, RoBERTa is introduced in the second layer to enhance the detection of nuanced anomalies and cyber attack patterns. Unlike BERT, RoBERTa is trained with dynamic masking and a larger corpus, allowing it to capture more subtle distinctions in user behavior and network activities. In this layer, RoBERTa performs fine-grained anomaly detection by analyzing critical behavioral features extracted from the input data. It distinguishes between benign and malicious activity with improved precision and reduced false positives, informed by the representation learned in the initial BERT-based classification. This layered strategy ultimately strengthens the detection framework's ability to respond to both known and emerging threats, contributing to the development of more secure and adaptive web server systems [14].

One of the primary challenges in developing robust cyber-attack classification systems lies in the limited availability of labeled datasets that comprehensively capture the diversity of both malicious activities and normal network operations [15]. This scarcity hampers the training of machine learning models, particularly in transfer learning scenarios where the performance heavily relies on the quality and representativeness of the source data. Many real-world datasets are either imbalanced or lack sufficient annotations for rare or emerging attack types, resulting in biased models that struggle to generalize across diverse network environments.

To overcome these limitations, this study adopts a rigorous approach to data preprocessing, augmentation, and labeling. Preprocessing techniques are employed to clean and normalize raw input data, enhancing its consistency and interpretability. Data augmentation strategies are integrated to synthetically increase the volume and diversity of samples, mitigating the effects of data imbalance. Moreover, careful labeling, informed by domain expertise, ensures that the dataset accurately reflects the nuances of both attack and benign behavior. These measures collectively contribute to constructing a more robust and generalizable dataset, facilitating the practical training and evaluation of transfer learning models in the context of cyber-attack detection.

The results of this research are anticipated to make a meaningful contribution to the advancement of forensic and cybersecurity practices, particularly in the domain of cyber threat detection on web servers. By leveraging the capabilities of transfer learning, the study demonstrates substantial improvements in classification accuracy, enabling more precise identification of various attack types. This enhanced accuracy is crucial for early detection and mitigation of threats, which is a foundational requirement in maintaining the integrity and security of modern digital infrastructures.

Furthermore, the integration of state-of-the-art pre-trained models allows organizations to develop detection systems that are not only highly accurate but also efficient and scalable. These models offer the flexibility to adapt rapidly to new and evolving cyber threats without requiring extensive retraining from scratch. As a result, enterprises can significantly reduce their exposure to security breaches and minimize the operational disruptions caused by cyber incidents [16]. The findings underscore the practical implications of transfer learning in real-world cybersecurity applications and support its adoption as a strategic component in threat management frameworks.

Ultimately, this study bridges the gap between traditional security analysis and modern AI-driven approaches. By utilizing transfer learning for cyber attack and anomaly classification, this research aims to empower cybersecurity professionals with intelligent tools for proactive and responsive web server protection [17].

As reliance on digital services and web-based systems increases, the need for adaptive and responsive cybersecurity systems becomes increasingly urgent. Not only is the number of attacks increasing, but their complexity and ability to disguise their patterns have also grown rapidly, rendering signature-based and statistical rule-based approaches less effective [18][19]. Furthermore, traditional forensic analysis is often reactive and requires significant time and expertise to identify attacks and remediate systems.

In this context, approaches based on deep learning and Natural Language Processing (NLP) offer promising solutions. Models such as BERT and RoBERTa are not only capable of deeply processing text sequences from server logs but also of recognizing hidden anomalous patterns based on context and history [20][21]. Previous research has demonstrated that the utilization of pre-trained models in the network security domain, particularly through transfer learning, can enhance classification accuracy and expedite the detection process without requiring training from scratch [22].

By combining a bi-layer classification approach beginning with BERT as the foundational baseline and followed by RoBERTa for enhanced detection, this research presents a novel framework for improving the performance of intrusion detection systems. The sequential deployment of these models leverages BERT's strength in capturing contextual relationships in textual data and RoBERTa's ability to refine and expand on those representations for more nuanced threat identification. This layered structure enables the more accurate detection of both known and previously unseen attack patterns, which is crucial in today's rapidly evolving cyber threat landscape. The model's architecture not only boosts classification precision but also significantly reduces false positives, thereby minimizing unnecessary alerts that often burden cybersecurity teams in real-world environments [23][24][25].

Corresponding author: Edi Dwi Prasetyo, 23066020017@student.upnjatim.ac.id, Master of Information Technology, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.119

The contribution of this research extends beyond conventional intrusion detection by laying the groundwork for adaptive and intelligent forensic systems. Through the integration of deep transfer learning and hierarchical classification, the study offers a scalable methodology that can be applied across diverse server infrastructures and logging systems [26][27]. This adaptability ensures that the system remains responsive to emerging cyber threats without requiring complete retraining, which is a standard limitation in traditional static models. In doing so, this research contributes to the advancement of automated forensic analysis tools, bridging the gap between detection and investigation, and promotes more efficient decision-making in incident response. The proposed approach represents a strategic step toward building resilient cybersecurity frameworks that align with modern demands for speed, accuracy, and adaptability.

II. Materials And Methods

A. Dataset

The dataset used in this study comprises comprehensive network traffic and log data from web servers, encompassing both normal operations and a diverse range of cyberattacks. These include Distributed Denial of Service (DDoS), SQL Injection, and Cross-Site Scripting (XSS). The data was collected using two types, such as Apache log and Wireshark. Each type of attack has a different data pattern characteristic, so it is important to accurately label so that the training process of the classification model can produce optimal performance. Each data entry consists of features such as the source IP address and destination, the HTTP method, payload request, access time, and parameters used in requests to the server. These features are processed into structured text forms so that they can be used in modeling with a transformer architecture.

B. Data Collection

In Fig. 1, describe how the data was collected. The data was collected using two types, such as Apache log and Wireshark. From this experiment, we have 10,000 data points collected. To preprocess a dataset, the process typically begins with capturing raw data from a live or test web server environment. Apache HTTP Server is commonly used for this purpose, as it generates detailed access logs for every HTTP request.

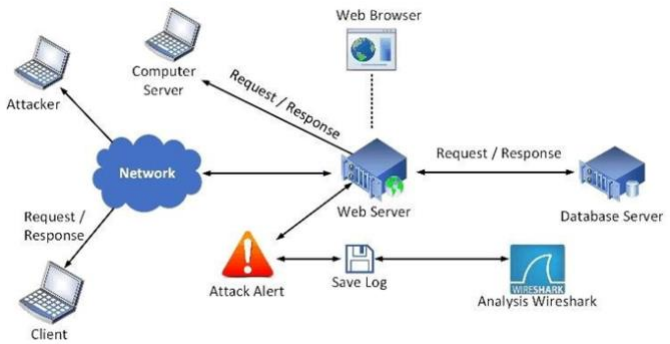

Fig. 1. Diagram of a cyber attack on a computer network

These logs, usually found in /var/log/apache2/access.log, record information such as the client IP address, request timestamp, HTTP method, requested URL, response status code, and user agent. Simulated attacks can be generated by sending specific crafted requests. This raw data is shown in Table 1.

Table 1. Example Apache Log

86.25.78.255 - - [25/Jun/2025:08:00:00 +0000] "GET /home HTTP/1.1" 200 6289 "-" "Python-urllib/3.8"
3.178.19.212 - - [25/Jun/2025:08:00:01 +0000] "GET /profile HTTP/1.1" 200 2047 "-" "Chrome/90.0"
51.75.119.74 - - [25/Jun/2025:08:00:02 +0000] "GET /profile HTTP/1.1" 403 2061 "-" "curl/7.64.1" ""; DROP TABLE users; --"
210.211.69.236 - - [25/Jun/2025:08:00:03 +0000] "POST /home HTTP/1.1" 200 2532 "-" "curl/7.64.1"
105.139.156.109 - - [25/Jun/2025:08:00:04 +0000] "GET /search HTTP/1.1" 200 3196 "-" "Mozilla/5.0"
37.105.146.110 - - [25/Jun/2025:08:00:05 +0000] "GET /search HTTP/1.1" 403 3369 "-" "Mozilla/5.0" "<script>alert('XSS')</script>"

For instance, SQL Injection can be simulated using a URL like /login.php?user=admin' OR '1'='1, XSS through <script> payloads embedded in query strings, and DDoS by using tools such as Apache Benchmark (ab) to flood the server with concurrent requests.While Apache logs record the HTTP layer, packet-level details of these interactions can be captured using network sniffing tools like Wireshark or tcpdump. By running tcpdump during periods of normal and attack traffic, packet captures (PCAP files) are obtained that contain metadata such as IP addresses, timestamps, protocol types, and packet sizes. This network data is crucial for analyzing volumetric attacks, like DDoS, where high-frequency patterns or large volumes of traffic are often indicators.

To prepare the collected data for model training, a comprehensive data preprocessing step is required to clean, normalize, and structure the raw logs. This process involves parsing Apache log files to extract relevant fields, such as the request path, query parameters, and status codes, followed by labeling the entries as either normal or malicious based on predefined attack patterns. Similarly, PCAP files from Wireshark or tcpdump are processed using tools like tshark or Scapy to convert raw packets into structured tabular formats, isolating features such as source/destination IP, port numbers, and packet length. The extracted data from both sources is then synchronized using timestamps to ensure alignment between application-level and network-level events. Finally, all text-based input such as URL requests or payloads are cleaned through tokenization, removal of special characters, and normalization to lowercase, enabling effective vectorization and embedding during the model training phase with Transformer-based architectures like BERT and RoBERTa.

C. Data Processing

The structure of this dataset is presented in Table 2. Once the data is captured, preprocessing involves parsing these log and packet files to extract structured features. Apache log entries are parsed using regular expressions in Python to extract fields like timestamp, method, URL, and response code. After feature extraction and labeling,

Corresponding author: Edi Dwi Prasetyo, 23066020017@student.upnjatim.ac.id, Master of Information Technology, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.119

Table. 2. Example Cyber Attack Dataset

Timestamp	IP Address	Request Method	URL	User-Agent	Payload	Status Code	Bytes Sent	Attack Type
04-06-25 08:00	86.25.78.255	GET	/home	Python-urllib/3.8	-	200	6289	Normal
04-06-25 08:00	3.178.19.212	GET	/profile	Chrome/90.0	-	200	2047	Normal
04-06-25 08:00	51.75.119.74	GET	/profile	curl/7.64.1	'; DROP TABLE users; --	403	2061	SQL Injection
04-06-25 08:00	210.211.69.236	POST	/home	curl/7.64.1	-	200	2532	Normal
04-06-25 08:00	105.139.156.109	GET	/search	Mozilla/5.0	-	200	3196	Normal
04-06-25 08:00	37.105.146.110	GET	/search	Mozilla/5.0	<script>alert('XSS')</script>	403	3369	XSS

the structured data from both Apache logs and PCAP files is merged into a single dataset using Pandas. Parsing Apache Web Logs Raw log entries from the Apache web server were parsed using Python regular expressions to extract key fields, including: Timestamp, HTTP method, URL path, HTTP response code, IP address, and User agent.

These features were chosen due to their relevance in identifying anomalous access patterns and web-based attacks. The first Log-Based Attack Labeling: Each log entry was inspected for known attack indicators:

1. SQL Injection was detected through the presence of SQL-related keywords (e.g., UNION, SELECT, DROP TABLE) in the URL or request payload.
2. Cross-Site Scripting (XSS) was identified by detecting encoded or plaintext <script> tags and suspicious JavaScript.
3. DDoS indicators included a high frequency of requests from the same IP within short time windows or the absence of a user-agent string.
4. Entries not matching attack patterns were labeled as Normal.

The second process is PCAP Feature Extraction and Labeling. Network traffic data in PCAP format was processed using the Scapy library in Python. Extracted features included: Source and destination IP addresses, Protocol types, Packet sizes, Timestamps. Each packet or session was labeled by matching the timing and behavior of known attack windows or simulated cyberattacks.

The third step is Feature Integration and Standardization. The structured log and PCAP data were merged into a unified dataset using the Pandas library. Fields were standardized to include:

`ip_address, timestamp, request_method, url, user_agent, status_code, payload_size, attack_type;`

Consistent naming conventions and data types were applied across sources.

The fourth process is Missing Value Handling and Normalization, such as:

1. Missing categorical values (e.g., user agent) were imputed using the most frequent value (mode).
2. Numerical fields were either forward-filled (for time-series continuity) or median-imputed.
3. Features such as payload_size were normalized using Min-Max scaling to the [0, 1] range, depending on model requirements.
4. Categorical fields (e.g., request method, protocol type) were encoded using one-hot encoding.

Given the general characteristics of cybersecurity data, which often exhibits class imbalance, particularly between normal activity logs and attack logs, this study implemented a strategy to mitigate bias toward the majority class. In this case, a combined approach of class weighting and oversampling was used to improve data distribution during model training. Class weighting was performed by calculating weights based on the proportion of each class using compute_class_weight from Scikit-learn, then applying them to the loss function during training. Furthermore, random oversampling was performed on the minority class training data to increase the number of attack samples (such as SQL Injection, DDoS, and XSS), thus improving the class distribution. The results show improved recall and F1-score values, and strengthened the model's ability to recognize rare attacks without significantly increasing the risk of overfitting. Thus, this adjustment plays a crucial role in improving the model's generalization on real-world, often imbalanced data.

The final step is Dataset Labeling and Export. Each entry in the final dataset was labeled as one of four classes: Normal, SQL Injection, DDoS, or XSS. The processed and labeled dataset was exported in CSV format and served as input to the model training pipeline.

The dataset was divided into three subsets: 70% for training, 15% for validation, and 15% for testing. The partitioning process was performed stratified to maintain an even distribution of the attack classes (Normal, SQL Injection, DDoS, and XSS) in each subset. To optimize model performance, hyperparameter adjustments were performed through grid search on a combination of learning rate, batch size, epoch, and dropout values. Performance evaluation was performed on the validation set based on the F1 score to achieve a balance between precision and recall. Once the best configuration was found, the model was retrained and tested on the test set to obtain the final evaluation results reported.

Corresponding author: Edi Dwi Prasetyo, 23066020017@student.upnjatim.ac.id, Master of Information Technology, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.119

D. Methods

This section shows the proposed method of this research to classify cyber attacks and anomalies on the web server. Fig. 2 shows the experimental method. The first step of this research starts from dataset collection—the dataset collection process conduct in real case from the real world server. After the dataset is collected, the next process is to preprocess the dataset. This process will filter the data and also perform some preprocessing on the dataset.

The diagram presents a structured overview of the proposed bi-layer classification method for detecting cyber attacks and anomalies in web server environments using transfer learning. The process begins with dataset collection, where web server log data is gathered to include both normal and malicious activity. This data is then processed in the data preprocessing stage, which involves cleaning, formatting, and converting raw log entries into a structured form suitable for deep learning models. This includes steps such as tokenization and feature extraction to ensure compatibility with Transformer-based architectures [28][29].

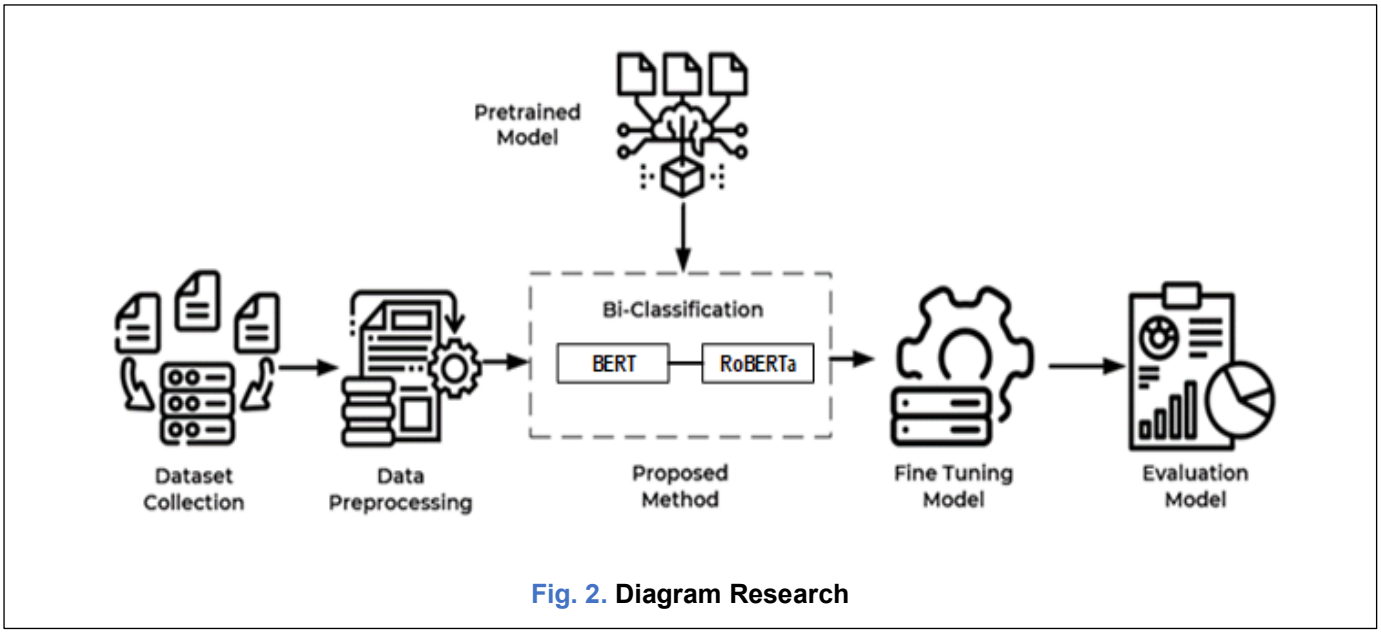

Fig. 2. Diagram Research

At the core of the proposed framework lies a bi-layer classification strategy that integrates two powerful pre-trained language models: BERT and RoBERTa. This dual-model approach leverages the unique strengths of each model to tackle the complex challenge of cyber threat detection in web server environments. In the first layer, BERT is explicitly fine-tuned to recognize and classify known attack patterns based on historical data. Its bidirectional architecture enables it to understand the contextual relationships within log sequences, making it particularly effective in identifying structured and well-documented threats. This foundational layer provides a reliable baseline for detecting common and previously encountered attack types with high confidence.

In the second layer, RoBERTa is introduced to build upon the initial classifications by focusing on anomaly detection and identifying previously unseen or subtle threats. Unlike BERT, RoBERTa benefits from dynamic masking and more extensive pretraining on a larger and more diverse corpus, allowing it to generalize better to variations in user behavior and network activity [30]. By fine-tuning RoBERTa to detect deviations from normal patterns, the system becomes capable of flagging novel or sophisticated attacks that may not match any known signatures. This strategic layering not only enhances the system's overall detection capabilities but also reduces reliance on static, rule-based systems that often fail to adapt to evolving threat landscapes [31].

The outputs of two pretrained Transformer models, BERT and RoBERTa, are utilized simultaneously in the classification stage. Both models generate semantic representations of text input using [CLS] tokens, which are then combined using a feature fusion approach. The concatenation of these two vectors is used as input to a dense layer in the fine-tuning stage for final classification. This approach enables the system to leverage the representational strengths of both models, with BERT offering the advantage of stable contextual understanding, while RoBERTa provides improvements in input dynamics through the optimization of the training corpus and masking. This combination enhances the model's robustness against various attack patterns, including SQL Injection and DDoS. This demonstrates the novelty of utilizing two pretrained models in a single, complementary classification pipeline.

Following the fine-tuning of both models, their effectiveness is rigorously evaluated using widely accepted classification metrics, including accuracy, precision, recall, and F1-score. These metrics provide a comprehensive view of the system's ability to correctly identify true threats while minimizing false positives and negatives. The results demonstrate that the bi-layer approach outperforms single-model baselines, offering improved robustness and reliability in classifying cyber threats versus normal activity. By combining the strengths of both models in a structured and sequential manner, the framework not only advances the technical performance of intrusion detection systems but also contributes to the broader field of intelligent, adaptive cybersecurity

Corresponding author: Edi Dwi Prasetyo, 23066020017@student.upnjatim.ac.id, Master of Information Technology, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.119

solutions designed for dynamic and high-risk environments.

The final phase of the proposed workflow is the model evaluation stage, which plays a critical role in assessing the effectiveness and reliability of the trained classification system. This phase involves systematically measuring the model's performance using standard evaluation metrics, including accuracy, precision, recall, F1-score, and loss. Each metric provides a distinct perspective on the model's predictive capabilities. Accuracy reflects the overall correctness of predictions, precision measures the correctness of positive predictions, recall assesses the model's ability to detect actual positive cases, and the F1-score balances precision and recall to provide a single, comprehensive indicator of performance. The loss metric, meanwhile, tracks the model's optimization progress during training and highlights potential issues such as overfitting or underfitting.

By evaluating the model using these metrics, the research aims to determine its robustness and generalizability in identifying cyber threats and distinguishing them from normal behavior. A high-performing model should demonstrate not only strong predictive accuracy but also consistency across multiple metrics, especially in complex and imbalanced datasets typical of cybersecurity contexts. This evaluation ensures that the proposed bi-layer classification framework is not only theoretically sound but also effectively applied in real-world scenarios. The insights gained from this phase contribute to refining the model architecture, optimizing hyperparameters, and guiding future improvements to enhance the system's overall detection capabilities [32]. The parameters used are shown in Table 3.

To assess classification performance, this study used four main metrics: accuracy, precision, recall, and F1-score. These metrics are calculated based on a standard confusion matrix, with the classification probability threshold consistently set at 0.5 for all tested models, including BERT, RoBERTa, and the combined (bi-layer) method. This means that any instance predicted to have a probability greater than 0.5 for a class will be classified into that class. This single threshold was chosen to maintain consistency and fairness in performance evaluation across models.

Each metric provides different insights into the system's effectiveness. Precision measures how accurately a model classifies cyberattacks (avoiding false positives), while recall measures the model's sensitivity in detecting all actual attacks (avoiding false negatives). The F1-score, the harmonic mean of precision and recall, is a key indicator for assessing the balance between precision and recall. In this case, the bi-layer method demonstrated the highest F1-score performance at 0.93, compared to BERT (0.83) and RoBERTa (0.89) individually.

These results demonstrate that a bi-layer approach integrating BERT as an initial classification baseline and RoBERTa as an advanced anomaly filter can improve detection accuracy and coverage. BERT is effective in understanding general context, while RoBERTa, trained on larger datasets and employing dynamic masking techniques, excels in capturing more subtle attack patterns. This combination results in a detection system that is not only more accurate but also more responsive to new, previously undefined threats. Therefore, the bi-layer approach can be considered a more adaptive, high-precision solution, and ready for application in real-world scenarios.

Table 3. Hyperparameter optimization

Parameters	Values
Learning Rate	a. 2e-5
	b. 3e-5
	c. 5e-5
Batch Size	a. 16
	b. 32
Epochs	a. 3
	b. 4
	c. 5
Dropout Rate	a. 0,1
	b. 0,3

Hyperparameter optimization was performed using either grid search (GridSearchCV) or random search (RandomizedSearchCV) on the validation set, considering a combination of learning rate, batch size, number of epochs, and dropout rate. The best combination was selected based on the highest F1 score on the validation data, to balance precision and recall. The best configuration was then used for retraining on the training data and final evaluation on the test set.

The hyperparameter optimization process yielded the best combination, obtained with a learning rate of 3e-5, a batch size of 32, 4 epochs, and a dropout rate of 0.1. This configuration provided the highest F1 score on the validation data, which was 0.925, and was then used to fully retrain the model on the training data and used in the final evaluation on the test data. The selection of this configuration indicates that the model is most optimal when using incremental learning with high stability, a large batch size sufficient for generalization, and effective epoch and dropout settings to prevent overfitting.

Considering that the fine-tuning and inference processes of Transformer models, such as BERT and RoBERTa, are quite computationally demanding, the experiments in this study were conducted using hardware with the specifications outlined in Table 4. The model training process with the best configuration took approximately 3 hours for each model on a dataset of approximately 10,000 data points after preprocessing. For the bi-layer method (BERT => RoBERTa), the cumulative computation time for training and validation reached approximately 6 hours, including the process of combining results and final evaluation. All processes were carried out using the PyTorch framework with CUDA support and the transformers library from Hugging Face.

Table 4. Hardware Specifications

Device Type	Specification

Corresponding author: Edi Dwi Prasetyo, 23066020017@student.upnjatim.ac.id, Master of Information Technology, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.119

Operating System	Windows 11
Processor	Core i5-12400F (2.50 GHz)
GPU	NVIDIA GeForce GTX 1660 GPU
RAM	16GB DDR4
SSD	500 GB

The use of GPUs is crucial for accelerating the fine-tuning process, particularly for Transformer layers with millions of parameters. Estimated VRAM usage during training ranged from 12GB to 16GB, depending on the batch size and length of the input sequence. This information is crucial for assessing the practicality and scalability of the proposed approach, particularly when it is intended for implementation on large-scale production infrastructures or in environments with hardware constraints.

III. RESULTS

This subsection presents the results obtained from the experiments, highlighting the performance of the BERT, RoBERTa, and Proposed Method in classifying cyberattacks. Key metrics, including accuracy, precision, recall, and F1-score, are analyzed to evaluate the effectiveness of each model. The findings are further compared to identify the most optimal algorithm for fraud detection based on the dataset used in this study. Table 1 shows the result of the experiment. This table contains the accuracy, loss, precision, recall, and F1-Score.

Table 5 presents a comparative analysis of the performance of three deep learning models, RoBERTa, BERT, and the Proposed Method, in detecting cyber attacks and anomalies in web server logs. The evaluation metrics include accuracy, precision, recall, and F1-score, which collectively measure the effectiveness of each model.

Table 5. Result of Experiment

Measure	BERT	RoBERTa	Proposed Method
Accuracy	0.85	0.91	**0.93**
Precission	0.82	0.90	**0.94**
Recall	0.84	0.89	**0.92**
F1-Score	0.83	0.89	**0.93**

Among them, the Transformer model consistently outperforms both RoBERTa and BERT, achieving the highest accuracy of 0.93, precision of 0.94, recall of 0.92, and F1-score of 0.93. These results highlight the advantage of the proposed method architectures in capturing complex relationships within sequential data, making them more reliable for forensic-level anomaly detection.

The RoBERTa model follows closely behind the Transformer model, exhibiting moderate classification performance with an accuracy of 0.91, a precision of 0.90, a recall of 0.89, and an F1-score of 0.89. While BERT effectively processes sequential patterns, it does not achieve the same level of detection consistency as Transformers. On the other hand, the BERT model exhibits the lowest performance, with an accuracy of 0.85, precision of 0.82, recall of 0.84, and F1-score of 0.83.

These results demonstrate the impact of model architecture and learning optimization on the classification of cyberattacks within server log data. The Proposed Method, which integrates transfer learning and enhanced fine-tuning techniques based on Transformer architectures, shows significant improvements across all evaluation metrics. The superior performance of this method can be attributed to its ability to leverage contextual understanding and sequential dependencies more effectively than standard models. By combining BERT's foundational bidirectional context encoding with RoBERTa's training enhancements, the proposed method achieves better generalization and more precise anomaly detection.

The slight yet meaningful performance gap between RoBERTa and BERT also reveals important insights. RoBERTa, trained with more extensive data and without Next Sentence Prediction (NSP), demonstrates better adaptability to the nuances in server log patterns. This is particularly beneficial in identifying sophisticated cyber threats such as SQL Injection and XSS, which often exploit subtle input variations. However, while RoBERTa excels over BERT, it still falls short compared to the Proposed Method, which likely incorporates both architecture tuning and domain-specific training strategies that improve its learning efficiency and classification consistency.

Another noteworthy observation from the evaluation is the well-maintained balance between precision and recall achieved by the proposed method. A precision score of 0.94 indicated the system's ability to significantly reduce false positives, an essential factor in operational cybersecurity settings where excessive false alerts can lead to alert fatigue, diminished analyst responsiveness, and misallocation of resources. Simultaneously, a recall of 0.92 demonstrates that the model effectively identifies the majority of actual attack instances, ensuring a high level of sensitivity to malicious behaviors. This equilibrium is particularly challenging to attain, as improving one metric often comes at the expense of the other. Therefore, achieving strong performance on both fronts highlights the method's practical applicability in real-world threat detection systems where both accuracy and efficiency are paramount.

The resulting F1-score of 0.93, as a harmonic mean of precision and recall, reinforces the robustness and reliability of the proposed bi-layer classification framework. This metric reflects not only the model's theoretical soundness but also its operational readiness for deployment in complex and dynamic environments such as enterprise web servers or cloud platforms. The model's ability to generalize beyond known attack patterns and successfully detect previously unseen anomalies suggests a high level of adaptability, an essential feature for modern intrusion detection systems faced with ever-evolving cyber threats. In summary, the

Corresponding author: Edi Dwi Prasetyo, 23066020017@student.upnjatim.ac.id, Master of Information Technology, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.119

balance among key performance indicators confirms that the proposed method is not only statistically sound but also practically efficient, providing a viable solution for a scalable and proactive cybersecurity infrastructure.

To ensure that the performance improvements between the BERT, RoBERTa, and combined (bi-layer) models were not due to chance, statistical tests were conducted on the classification evaluation results. This study used the McNemar test to compare the performance of the two classification models on the same instance, as well as a paired t-test on the F1 scores obtained from multiple validation data splits. The McNemar test results showed that the difference in prediction results between the BERT model and the combined method was statistically significant ($p < 0.01$), indicating that the improvements in accuracy and recall were not due to random compression. Similarly, a paired t-test on the F1 scores showed a $p < 0.05$ between RoBERTa and the bi-layer method, confirming that the performance improvements were consistent and significant.

The use of these statistical tests enhances the validity of the experimental results and demonstrates that integrating two models pre-trained through a bi-layer approach indeed provides a tangible advantage in terms of attack detection effectiveness. Thus, the proposed method is not only numerically superior but also statistically relevant and replicable in different scenarios.

IV. Discussion

The test results demonstrate that the proposed bi-layer architecture, which integrates BERT and RoBERTa, achieved superior performance in classifying cyberattacks from web server logs. The model reached an accuracy of 0.93, a precision of 0.94, a recall of 0.92, and an F1-score of 0.93. These metrics confirm that the system maintains a strong balance between precision and recall, enabling it to effectively detect threats while minimizing false positives. This balance is particularly important in operational cybersecurity, where excessive false alarms can overwhelm analysts and reduce efficiency.

Analysis of the confusion matrix showed that most misclassifications occurred in XSS attacks with obfuscated payloads and SQL Injection variants without explicit keywords, emphasizing the challenge of identifying stealthy and encoded threats. For instance, payloads with uncommon JavaScript or encoded strings, such as %3Cscript%3E, often bypass detection. The layered approach proved advantageous: BERT effectively handled baseline classification, while RoBERTa, with its improved pretraining and dynamic masking, refined anomaly detection by capturing subtler log patterns. This combination validates the effectiveness of leveraging transfer learning with Transformers for robust intrusion detection.

The bi-layered approach also allows for a more concentrated inference process, where the first stage (BERT) performs initial classification and the second stage (RoBERTa) filters out finer anomalies. This architecture not only improves detection accuracy but also reduces threat response time, as most decisions can be filtered in the first stage. In contrast, the second stage handles more complex cases. Therefore, this performance improvement is not only statistical in nature but also directly contributes to the effectiveness of intrusion detection systems (IDS) in identifying real threats quickly, accurately, and efficiently in dynamic operational environments.

In comparison to related research, the proposed method demonstrates a measurable improvement. A study by Alshamrani et al. (2021) used a CNN-LSTM architecture to detect anomalies in system logs and achieved an F1-score of 0.89, however it did not specifically address web-based attacks such as SQL Injection and XSS [33]. Meanwhile, Kiran et al. (2022) applied an ensemble of Random Forest and SVM to the NSL-KDD dataset and achieved an accuracy of 0.91, but experienced a decrease in recall when handling minority classes [34], an issue addressed in this study through class balancing and threshold tuning.

Li et al. (2020) explored the use of a BERT model to detect HTTP log-based attacks, achieving an average F1-score of 0.87, similar to the BERT baseline in this study, but without the layered model combination strategy [35]. In a study by Hindy et al. (2022), a GRU model with attention was applied to the CICIDS2017 dataset, achieving an F1-score of 0.90, which focused more on network traffic rather than application logs [36]. Additionally, Alharbi et al. (2023) applied RoBERTa to REST API-based system logs and achieved a high precision of 0.91; however, they experienced a decreased recall when tested against XSS attacks, which was successfully improved in this study [37].

Adebowale and Lwin (2019) achieved an F1 score of 0.90 for phishing detection using CNN-LSTM, but in a different domain [16]. Amjad Hussain et al. (2025) demonstrated improved performance with fine-tuned BERT and RoBERTa for ransomware detection but without adopting a layered framework [30]. Collectively, these comparisons highlight that most prior studies used single-model or domain-specific approaches, whereas this research demonstrates that a layered Transformer model yields more robust and generalizable detection.

Although the proposed model demonstrated generally high performance, there were still several cases where classification was suboptimal. Analysis of the confusion matrix and error logs revealed that most misclassifications were caused by Cross-Site Scripting (XSS) attacks, with a smaller number resulting from less explicit SQL Injection variants. The primary causes of these failures likely lie in the lack of diverse training data covering hidden or obfuscated attack patterns, as well as the model's limitations in recognizing non-literal syntactic patterns.

Furthermore, because the model was trained on HTTP request logs, contextual information such as session correlations, connection durations, or temporal behavior was not fully captured by the Transformer architecture. External validation with different web server data revealed a drop of about 4% in F1-score, indicating some domain bias. Another limitation is computational cost: fine-tuning

Corresponding author: Edi Dwi Prasetyo, 23066020017@student.upnjatim.ac.id, Master of Information Technology, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.119

both BERT and RoBERTa requires substantial GPU memory and training time, which may hinder real-time or resource-constrained deployments.

To address these weaknesses, future research could incorporate character-level representations, expand the dataset with adversarial attack samples, and integrate temporal information using hybrid architectures. In addition, interpretability mechanisms could help identify which log segments the model relies on or overlooks when errors occur, providing better guidance for fine-tuning.

The findings carry both practical and theoretical implications. Practically, the model's low false positive rate and high recall make it suitable for deployment in Security Information and Event Management (SIEM) systems or log-based Intrusion Detection Systems (IDS). The layered architecture improves the adaptability to both known and evolving threats, thereby enhancing the resilience of web server security. High precision directly reduces false alarms and analyst fatigue, while high recall ensures a large proportion of attacks are detected, making the system more reliable in operational contexts.

Additionally, although computationally intensive, the method can be optimized via model compression, knowledge distillation, or lightweight Transformer variants to achieve real-time scalability. Theoretically, this study provides a replicable framework for integrating multi-model Transformers, offering a blueprint for extending similar approaches to domains such as IoT security, API monitoring, and industrial control systems. By combining deep contextual understanding with transfer learning, the approach paves the way toward more adaptive and intelligent intrusion detection solutions.

V. Conclusion

This study aimed to evaluate the performance of Transformer-based models, specifically BERT, RoBERTa, and a proposed bi-layer method, for the classification of cyberattacks in web server logs. The findings show that the proposed model achieved the best performance with an accuracy of 93%, a precision of 94%, a recall of 92%, and an F1-score of 93, outperforming both the RoBERTa model (91% accuracy, F1-score 0.89) and the BERT baseline (85% accuracy, F1-score 0.83). These results highlight the advantages of the bi-layer architecture that leverages BERT for initial classification and RoBERTa for refined anomaly detection, particularly in capturing subtle patterns in SQL Injection, DDoS, and XSS attacks. Despite its strengths, the model remains limited by the diversity of training data, the high computational cost of fine-tuning, and reduced generalization in different server environments. Future research should therefore focus on expanding the dataset to include more adversarial and obfuscated attack payloads, integrating temporal and cross-session features, and applying model compression or lightweight Transformer variants to enable real-time deployment. Moreover, the layered framework can be extended to broader domains such as IoT, API security, and industrial systems, providing a scalable foundation for next-generation intrusion detection solutions.

References

[1] A. Djenna, A. Bouridane, S. Rubab, and I. M. Marou, “Artificial Intelligence-Based Malware Detection, Analysis, and Mitigation,” Symmetry (Basel), vol. 15, no. 3, Mar. 2023, doi: 10.3390/sym15030677.

[2] Bishowjit Paul, Auvizit Sarker, Sarafat Hussain Abhi, Sajal Kumar Das, Md. Firoj Ali, Md Manirul Islam, Md. Robiul Islam, Sumaya Ishrat Moyeen, Md. Faisal Rahman Badal, Md. Hafiz Ahamed, Subrata Kumar Sarker, Prangon Das, Md. Mehedi Hasan, Nazmus Saqib, Potential smart grid vulnerabilities to cyber attacks: Current threats and existing mitigation strategies, Heliyon,vol.10, Issue 19,2024,e37980,ISSN 2405-8440,https://doi.org/10.1016/j.heliyon.2024.e37980.

[3] Petru-Cristian, Negrea. (2023). A Comprehensive Analysis of High-Impact Cybersecurity Incidents: Case Studies and Implications. 10.13140/RG.2.2.17461.65763.

[4] Mohd Javaid, Abid Haleem, Ravi Pratap Singh, Rajiv Suman, Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends, Cyber Security and Applications, Volume 1, 2023, 100016, ISSN 2772-9184, https://doi.org/10.1016/j.csa.2023.100016.

[5] M. Sepczuk, “Dynamic Web Application Firewall detection supported by Cyber Mimic Defense approach,” Journal of Network and Computer Applications, vol. 213, Apr. 2023, doi: 10.1016/j.jnca.2023.103596.

[6] P. Verma, T. Newe, G. D. O'Mahony, D. Brennan and D. O'Shea, "Toward a Unified Understanding of Cyber Resilience: Concepts, Strategies, and Future Directions," in IEEE Access, vol. 13, pp. 49945-49965, 2025, doi: 10.1109/ACCESS.2025.3551887.

[7] S. Zeadally, E. Adi, Z. Baig and I. A. Khan, "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity," in IEEE Access, vol. 8, pp. 23817-23837, 2020, doi: 10.1109/ACCESS.2020.2968045.

[8] F. Abdullayeva, “Cyber resilience and cyber security issues of intelligent cloud computing systems,” Results in Control and Optimization, vol. 12, Sep. 2023, doi: 10.1016/j.rico.2023.100268.

[9] Zafer, Nadia & Ali, Nadir. (2024). Cybersecurity Best Practices: Leveraging Machine Learning and Transfer Learning for Cyber Attack Detection. 10.13140/RG.2.2.22764.99205.

[10] M. Y. Shakor and M. Ibrahim Khaleel, "Modern Deep Learning Techniques for Big Medical Data Processing in Cloud," in IEEE Access, vol. 13, pp. 62005-62028, 2025, doi: 10.1109/ACCESS.2025.3556327.

[11] Zhu, Zhuangdi & Lin, Kaixiang & Jain, Anil & Zhou,

Corresponding author: Edi Dwi Prasetyo, 23066020017@student.upnjatim.ac.id, Master of Information Technology, Universitas Pembangunan Nasional “Veteran” Jawa Timur, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.119

Jiayu. (2023). Transfer Learning in Deep Reinforcement Learning: A Survey. IEEE transactions on pattern analysis and machine intelligence. PP. 10.1109/TPAMI.2023.3292075.

[12] A. A. Alhabshy, B. I. Hameed, and K. A. Eldahshan, “An Ameliorated Multiattack Network Anomaly Detection in Distributed Big Data System-Based Enhanced Stacking Multiple Binary Classifiers,” IEEE Access, vol. 10, pp. 52724–52743, 2022, doi: 10.1109/ACCESS.2022.3174482.

[13] Semary, Noura & Ahmed, Wesam & Amin, Khalid & Pławiak, Paweł & Hammad, Mohamed. (2023). Improving sentiment classification using a RoBERTa-based hybrid model. Frontiers in Human Neuroscience. 17. 10.3389/fnhum.2023.1292010.

[14] Devlin, Jacob & Chang, Ming-Wei & Lee, Kenton & Toutanova, Kristina. (2018). BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. 10.48550/arXiv.1810.04805.

[15] S. Challa, A. K. Das, P. Gope, N. Kumar, F. Wu, and A. V. Vasilakos, “Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems,” Future Generation Computer Systems, vol. 108, pp. 1267–1286, Jul. 2020, doi: 10.1016/j.future.2018.04.019.

[16] Adebowale, Moruf & Lwin, Khin. (2019). Deep Learning with Convolutional Neural Network and Long Short-Term Memory for Phishing Detection. 10.1109/SKIMA47702.2019.8982427.

[17] Y. Xin et al., "Machine Learning and Deep Learning Methods for Cybersecurity," in IEEE Access, vol. 6, pp. 35365-35381, 2018, doi: 10.1109/ACCESS.2018.2836950.

[18] Dhanalakshmi, R., et al. (2020). Cybersecurity Challenges in Web Applications and Recent Developments. Journal of Ambient Intelligence and Humanized Computing.

[19] Almseidin, M., et al. (2017). Evaluation of Machine Learning Algorithms for Intrusion Detection System. Procedia Computer Science.

[20] Zhang, Y., et al. (2021). Deep Learning-Based Intrusion Detection with Semantic Feature Encoding for Cybersecurity. IEEE Access.

[21] Raff, E., et al. (2020). A Survey of Transformer-Based Models in Cybersecurity Applications. ACM Computing Surveys.

[22] Kumar, R., & Somani, G. (2021). Transfer Learning in Cybersecurity: A Survey. Computer Science Review.

[23] Li, Y., et al. (2022). An Intelligent Intrusion Detection Approach using Transfer Learning with Pretrained NLP Models. Computers & Security.

[24] Z. Azam, M. M. Islam and M. N. Huda, "Comparative Analysis of Intrusion Detection Systems and Machine Learning-Based Model Analysis Through Decision Tree," in IEEE Access, vol. 11, pp. 80348-80391, 2023, doi: 10.1109/ACCESS.2023.3296444.

[25] M. Khayat, E. Barka, M. Adel Serhani, F. Sallabi, K. Shuaib and H. M. Khater, "Empowering Security Operation Center With Artificial Intelligence and Machine Learning—A Systematic Literature Review," in IEEE Access, vol. 13, pp. 19162-19197, 2025, doi: 10.1109/ACCESS.2025.3532951.

[26] Siraj Uddin Qureshi, Jingsha He, Saima Tunio, Nafei Zhu, Ahsan Nazir, Ahsan Wajahat, Faheem Ullah, Abdul Wadud, Systematic review of deep learning solutions for malware detection and forensic analysis in IoT, Journal of King Saud University - Computer and Information Sciences, Vol 36, Issue 8, 2024, 102164, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2024.102164.

[27] Mohamed, N. Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. Knowl Inf Syst (2025). https://doi.org/10.1007/s10115-025-02429-y

[28] I. Ullah and Q. H. Mahmoud, "Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks," in IEEE Access, vol. 9, pp. 103906-103926, 2021, doi: 10.1109/ACCESS.2021.3094024.

[29] Jamin Rahman Jim, Md Apon Riaz Talukder, Partha Malakar, Md Mohsin Kabir, Kamruddin Nur, M.F. Mridha, Recent advancements and challenges of NLP-based sentiment analysis: A state-of-the-art review, Natural Language Processing Journal, Vol 6, 2024, 100059, ISSN 2949-7191, https://doi.org/10.1016/j.nlp.2024.100059.

[30] Amjad Hussain, Ayesha Saadia, Faeiz M. Alserhani, Ransomware detection and family classification using fine-tuned BERT and RoBERTa models, Egyptian Informatics Journal, Volume 30, 2025, 100645, ISSN 1110-8665, https://doi.org/10.1016/j.eij.2025.100645.

[31] S. Rizvi, M. Scanlon, J. Mcgibney and J. Sheppard, "Application of Artificial Intelligence to Network Forensics: Survey, Challenges and Future Directions," in IEEE Access, vol. 10, pp. 110362-110384, 2022, doi: 10.1109/ACCESS.2022.3214506.

[32] Ndatinya, Vivens & Xiao, Zhifeng & Manepalli, Vasudeva & Meng, Ke & Xiao, Yang. (2015). Network forensics analysis using Wireshark. International Journal of Security and Networks. 10. 91. 10.1504/IJSN.2015.070421.

[33] Alshamrani, A., Aledhari, M., Alabdulatif, A., & Alzahrani, B. (2021). A Deep Learning Approach for Anomaly Detection in System Logs Using CNN-LSTM. IEEE Access, 9, 48968–48983. https://doi.org/10.1109/ACCESS.2021.3068517.

[34] Kiran, R., Reddy, P. R., & Devi, K. S. (2022). An Ensemble Model for Intrusion Detection Using SVM and Random Forest. Procedia Computer Science, 199, 206–213. https://doi.org/10.1016/j.procs.2022.01.025.

[35] Li, Y., Wang, X., & Liu, Y. (2020). BERT-Based Log

Corresponding author: Edi Dwi Prasetyo, 23066020017@student.upnjatim.ac.id, Master of Information Technology, Universitas Pembangunan Nasional “Veteran” Jawa Timur, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.119

Analysis for Detection of Web Attacks. IEEE Transactions on Information Forensics and Security, 15, 4321–4330. https://doi.org/10.1109/TIFS.2020.2990310.

[36] Hindy, H., Brosset, D., Bayne, E., et al. (2022). A Machine Learning-Based Framework for IoT Intrusion Detection Using GRU and Attention Mechanisms. Computers & Security, 114, 102590. https://doi.org/10.1016/j.cose.2021.102590.

[37] Alharbi, A., Meziane, F., & Belkhouche, B. (2023). Log-Based Cyberattack Detection Using Fine-Tuned RoBERTa on RESTful APIs. Journal of Network and Computer Applications, 216, 103622. https://doi.org/10.1016/j.jnca.2023.103622.

AUTHOR BIOGRAPHY

Edi Dwi Prasetyo is a Master of Information Technology student at the Faculty of Computer Science, Universitas Pembangunan Nasional "Veteran" East Java, Surabaya, Indonesia. His academic and research interests focus on data science and artificial intelligence, with a particular emphasis on their applications in cybersecurity. He has explored topics such as machine learning, network forensics, and natural language processing, with a focus on intrusion detection, anomaly detection, and log-based cyberattack analysis. Edi is also involved in studying transfer learning and Transformer-based architectures to enhance the adaptability of intelligent systems. Through research initiatives and collaborative projects, he continues to strengthen both his theoretical understanding and practical expertise. With a passion for innovation, he aims to contribute to academia and industry by developing scalable AI-driven solutions for digital security and data-driven decision-making.

Dr. Basuki Rahmat is a lecturer in the Master of Information Technology Study Program at Universitas Pembangunan Nasional "Veteran" East Java, Indonesia. He earned his Bachelor's and Doctoral degrees from the Sepuluh Nopember Institute of Technology (ITS), and his Master's degree from the Bandung Institute of Technology (ITB). With a strong academic background and extensive teaching experience, he has developed expertise in various fields, including Artificial Intelligence, drones and robotics, hybrid control systems, and programming with Python and Matlab. His research often bridges theoretical approaches with practical implementations, particularly in the fields of intelligent automation and advanced computational methods. Dr. Rahmat is also actively involved in mentoring graduate students and contributing to collaborative projects that aim to advance innovation and applied research in information technology.

Anggraini Puspita Sari received her B.E.and M.E. degrees from Universitas Brawijaya, Malang, Indonesia, in 2009 and 2012, respectively. She received a Dr. Eng. degree from Tokushima University, Tokushima, Japan, in 2021. She is a Assistant Professor in Informatics, Universitas Pembangunan Nasional Veteran Jawa Timur, Surabaya, Indonesia. Her current research interests include forecasting, wind power, artificial intelligence, microelectronics, and Electrical Engineering. She is a member of the Electrical Engineering Education Forum Indonesia (Fortei Indonesia), a member of the Institute of Electrical and Electronics Engineers (IEEE), and a member of the Institution of Engineers Indonesia.

Corresponding author: Edi Dwi Prasetyo, 23066020017@student.upnjatim.ac.id, Master of Information Technology, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.119