Scientific Journal of Informatics
Vol. 11, No. 1, Feb 2024

p-ISSN 2407-7658 http://journal.unnes.ac.id/nju/index.php/sji e-ISSN 2460-0040

Analysis of Attack Detection on Log Access Servers Using Machine Learning Classification: Integrating Expert Labeling and Optimal Model Selection

Mohammad Ridwan[1*], Irwan Sembiring[2], Adi Setiawan[3], Iwan Setyawan[4]
[1]Department of Information System, Faculty of Engineering, Universitas Islam Syekh Yusuf Tangerang, Indonesia
[1,2,3,4]Computer Science Doctoral Department, Faculty of Science and Mathematics,
Universitas Kristen Satya Wacana Salatiga, Indonesia

Abstract.
Purpose: As the complexity and diversity of cyberattacks continue to grow, traditional security measures fall short in effectively countering these threats within web-based environments. Therefore, there is an urgent need to develop and implement innovative, advanced techniques tailored specifically to detect and address these evolving security risks within web applications.
Methods: This research focuses on analyzing attack detection in log access servers using machine learning classification with two primary approaches: expert labeling integration and best model selection. Expert labeling determines whether log entries are safe or indicate an attack.
Result: Validation in labeling was applied using different datasets to minimize errors and increase confidence in the resulting dataset. Experimental results show that the Decision Tree and Random Forest models have nearly identical accuracy rates, around 89.3%-89.4%, while the ANN model has an accuracy of 81%.
Novelty: This study proposes a fusion of expert knowledge in labeling log entries with a rigorous process of selecting the best classification model. This integration has not been extensively explored in previous research, offering a novel approach to enhancing attack detection within web applications. The research contribution lies in the integration of expert security assessment and the selection of the best model for detecting attacks on server access logs, along with validating labels using various datasets from different log devices to enhance confidence in the analysis results.

Keywords: Intrusion detection, Log server, Machine learning, Expert labeling, Best model selection
Received December 2023 / **Revised** February 2024 / **Accepted** February 2024

INTRODUCTION

In an increasingly complex digital era, the security of web applications has become highly critical due to the evolving and diverse nature of cyberattacks. Server logs, as primary sources of application activity-related information, play a key role in the effort to detect and prevent attacks. However, challenges arise in distinguishing between normal and suspicious activities within typically large and heterogeneous server logs [1], [2], [3].

The success of attacks on web applications can result in significant negative impacts, including financial losses, exposure of sensitive data, and harm to an organization's reputation. Therefore, swift and accurate attack detection is crucial to safeguarding web applications and user data. Traditional attack detection methods often encounter limitations in recognizing newly emerging or more sophisticated attack patterns, necessitating a more adaptive and intelligent approach [4]. This research explores harnessing the potential of classification to enhance the accuracy of attack detection within server logs [5], [6], [7].

One of the key parameters related to attacks is the server access log, a record of all user accesses requesting services from the web server. Server logs often contain heterogeneous data comprising various types of activities and events, making log data management and analysis complex. Intelligent approaches are needed

[*]Corresponding author.
Email addresses: mridwan@unis.ac.id (Ridwan)
DOI: 10.15294/sji.v11i1.49424

to discern between normal and suspicious activities [8], [9]. Thus, expert knowledge is required to determine whether a log entry is secure or indicates an attack [7][2], [10], [11].

Emphasis on the significance of web application security in the complex digital era can be found in works such as [12]. These studies outline the impacts of cyberattacks on web applications, encompassing financial losses and reputational damage to organizations. Web application security addresses vulnerabilities at the web application level, underscoring the importance of information security due to increased information exchange via the web. It analyzes common web vulnerabilities and provides best practices to prevent security issues throughout the development lifecycle [13]. Characteristics of software developers, such as application security awareness and self-efficacy, influence their information security behavior. Enhancing developers' awareness and self-efficacy can improve their information security behavior [14]. Web applications are susceptible to cyber-based attacks, and various security techniques have been developed to protect them. Prevention involves tool utilization, implementing security standards, and regularly assessing risk factors [1][15][16].

The analysis of server logs plays a crucial role in attack detection as it helps identify potential attacks and malicious activities [17]. These logs contain information about each request made to the web server, including details like the uniform resource identifier (URI), status codes, and user behavior. Through log analysis, machine learning systems can identify patterns and characteristics related to attacks, such as rapid crawling, numerous error status codes, and unusual user behavior. Log-based intrusion detection systems detect attacks by comparing recorded information with known attack signatures or by identifying anomalies in user behavior. Log analysis can also be used for real-time detection of streaming attack behaviors, enabling timely attack discovery. Overall, server logs provide valuable data for detecting and preventing attacks on web applications [18].

Web attack detection faces several challenges in today's technological environment. Traditional security measures, such as firewalls and encryption, have limitations in fully safeguarding web-based systems [19]. Additionally, evolving threats and cybercriminal behavior present difficulties in adapting systems and networks to effectively detect attacks [20]. To overcome these challenges, a new generation of web application firewall systems (WAF) is being developed using machine learning and deep learning technology [21]. These techniques can autonomously learn without human intervention and handle multidimensional data more effectively [22]. Distributed training processes that maintain privacy have also been proposed to enhance accuracy while preserving local data and model parameters as secrets. However, the complexity of server log data poses a unique challenge, where automated approaches struggle to control log changes at every time interval, requiring specific understanding and knowledge to identify log developments [19]. The heterogeneity and complexity of server log data demand intelligent approaches to differentiate between normal and suspicious activities. In this context, this research explores the integration of expert labeling to enhance human interpretation.

Role of Expert Labeling: Implementing expert labeling in attack detection, as discussed in [11], serves as the foundation for involving security experts in labeling server log data. This is necessary to address the limitations of automated labeling. Expert labeling plays a crucial role in providing reliable and accurate information across various domains, and experts are considered trustworthy sources in complex systems such as the global food system [23]. Expert labels are often chosen as the most reliable source compared to other commonly used label types[24]. Their expertise helps improve labeling accuracy, even when dealing with mostly low-quality labels in crowdsourcing [25]. Collaborative labeling work with domain experts involves principled design, iterative design, and improvisational design, contributing to the quality of ground truth data [26]. In the context of machine learning, domain experts provide ground truth labels used to train models and enhance prediction accuracy [10]. Overall, expert labeling plays a crucial role in ensuring the reliability and quality of labeled data across various domains.

The development concept of machine learning classification models for attack detection within server logs has been explored in several papers. These models utilize deep learning techniques, such as DCGAN and ResNet-50, for feature extraction, and an AlexNet-based classifier optimized for network attack detection. The proposed approach achieved high accuracy rates, with an accuracy of 99.4% for the first public dataset and an accuracy 99.33% for the second dataset [27]. Another approach utilized an Extra Tree classifier in combination with Decision Tree, XGBoost, and Random Forest algorithms for DDoS attack detection [3]. Additionally, XGBoost Classifier and Random Forest were employed in modified forms to enhance model accuracy [28], [29]. All these studies focus on computer network attack detection using network transmission logs. There are several articles related to web attack detection applying machine learning within them. One example is by Eunaicy, who successfully developed an RNN with web logs (not server logs) and achieved an accuracy of 94% [22]. Furthermore, Alaoui used an HTTP Web Request dataset with the LSTM method, averaging 78% accuracy [30]. Riera also utilized a multi-label SR-BH 2020 dataset with the CatBoost algorithm achieving 88% accuracy [31]. However, all these related studies used outdated open-source datasets, raising uncertainties about the validity of these datasets in today's web security landscape. A new approach is needed to contribute to the latest datasets and validate the classification labeling using experts.

This study develops a machine learning classification model to enhance the accuracy of attack detection within server logs. The objective is to establish a more effective system for identifying new and advanced attack patterns. Integrating expert labeling into the attack detection process aims to provide a deeper human context and understanding of the recorded activities within server logs. The research contributes by creating the latest web server log dataset validated by experts, integrating expert security assessment, selecting the best model for detecting attacks on server access logs, and validating labels using various datasets from different log devices to enhance confidence in the analysis results.

METHODS

This section outlines the procedures used in the study to integrate expert security assessment and the best classification model for detecting attacks on server access logs. The flowchart of this process is depicted in Figure 1.

The research flowchart in Figure 1 encompasses several key steps. Firstly, data collection involves gathering server access logs from various sources and different log devices. Subsequently, the dataset undergoes preprocessing using transformation and cleaning techniques to create a refined dataset. Expert labeling by security professionals assesses log entries and validates labels, determining whether they represent safe activities or potential attacks based on their knowledge of attack patterns. Following that, the best model selection involves processing multiple machine learning classification models using specific criteria, such as accuracy and performance, to choose the optimal model for analysis. The validation process includes validating the dataset logs from various log devices to confirm the accuracy of the expert labeling process. The analysis results are then utilized to identify attacks and potential attack patterns within the server access log data. Through the integration of expert labeling, best model selection, and label validation, confidence in the analysis results is expected to increase, enabling more accurate decision-making in addressing cybersecurity threats.

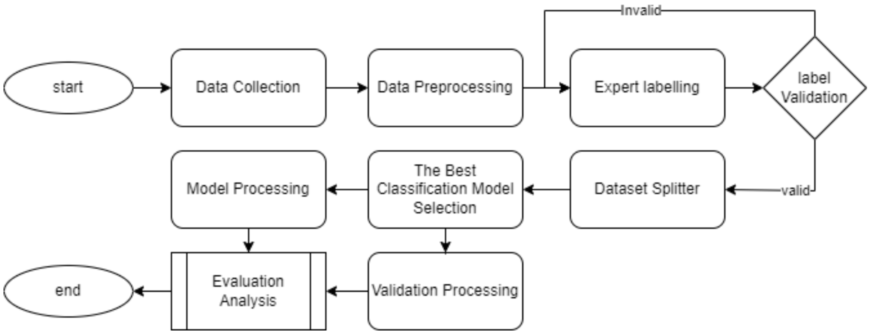

Figure 1. Research Flowchart

Figure 2 illustrates the data analysis process on a server log dataset comprising 27,729 rows and 6 attributes, entailing a series of crucial preprocessing steps. The initial step involves data transformation, where log sentences are split into several relevant attributes such as IP address, date, request, ID process, and from, to facilitate information representation. Subsequently, the data cleansing process removes empty values, handles duplicates, and normalizes data to ensure accuracy and consistency for further use. Next, security experts or rules, involving four experts, are assigned to label each data row as 'attack' or 'normal,' aiding in the classification process.

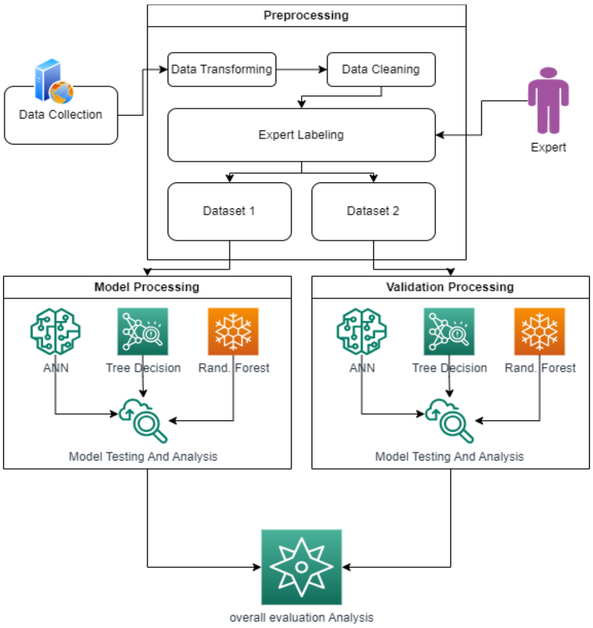

Figure 2. Research Analysis Framework

Once the dataset is prepared, the next step involves splitting it into two parts: 70% for model training and 30% for validation. In the modeling phase, three distinct methodologies are employed: Artificial Neural Network (ANN), Decision Tree for explicit rule representation, and Random Forest as a method that aggregates decision trees. Each model is trained with the training dataset and evaluated with the validation dataset to measure its performance and classification ability. Eventually, the results of testing these three models are compared using appropriate evaluation metrics to select the best model most suitable for the classification task between attacks and normal activities within the provided dataset. The chosen approach must be supported with citations, and any pertinent adjustments should be clearly elucidated. An in-depth examination of the procedure and data analysis methodology is imperative in a literature review manuscript. It is essential to provide comprehensive explanations of the research stages and analyses.

Artificial Neural Network (ANN): ANN consists of interconnected processing units known as neurons arranged in layers. Each neuron receives input, undergoes precise mathematical operations, and generates an output that then becomes input for subsequent neurons. This iterative process continues until the final outcome is achieved. ANN is capable of analyzing intricate patterns in data and identifying nonlinear correlations among pertinent attributes, facilitating the prediction of attack detection [5], [32], [33].
The general formula for a single neuron in an artificial neural network is:

$$Output = f\ (\textstyle\sum_{i}^{n} W_i\ x\ I_i +\ B), \tag{1}$$

where:
- Output is the neuron of output.
- *f* is the function of activation.
- W_i is the weight assigned.
- I_i is the input.
- *B* is the bias value.
- *n* is the number of inputs.

Random Forest (RF): A Random Forest is an ensemble learning technique that operates by constructing a multitude of decision trees. Each tree within the RF is trained using a randomly selected data subset, and the ultimate decision is predominantly influenced by the decisions taken by these trees. This technique addresses the constraints encountered with a single Decision Tree, including issues such as overfitting and potential bias of the dataset. RF enhances predictive power by amalgamating insights from multiple decision trees, resulting in robust and precise predictions [34], [35], [36]. The RF algorithm begins with random sample selection, decision-tree construction, and voting or averaging to generate a final prediction.

Decision Tree (Tree): A decision tree is a type of decision-making model with a tree-like structure. The goal is to iteratively partition the dataset according to established decision rules and minimize the impurities within each segment. The ultimate decision of the tree is made at the leaf nodes. Decision trees provide easily understandable decision rules and can discern significant features for predicting student academic performance [37], [38].

Gini impurity: If we have K classes, *p1*, *p2*, ..., *pK* are the proportions of each class in that node. Next is the Best Feature Selection, Splitting Rule, Tree Formation, and prediction, so that the result is the class or value generated from the leaf node where the data end.

RESULTS AND DISCUSSIONS

The experimental results are discussed in this section. First, we present the percentage comparison of target attributes can be shown in Figure 3.

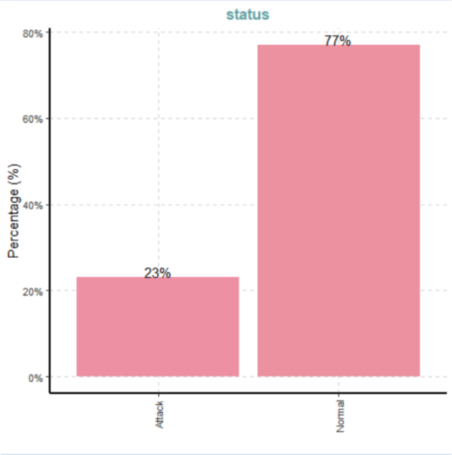

Figure 3. Percentage of Target Attributes

The dataset was compiled with normal status data accounting for 77% of the dataset, compared to attack data, which comprises only 23%. For further clarification, refer to Figure 3.

Table 1. Performance Results of the Proposed Model

Model	Recall	Precision	F-measure	Accuracy
ANN	0.603	0.9	0.61	0.81
Tree	0.809	0.885	0.838	0.893
RF	0.809	0.886	0.838	0.894

Based on the performance evaluation results of the three models tested in Table 1, it is observed that the ANN achieved an accuracy of 81%, with a recall of 60.3%, precision of 90%, and an F-measure of 61%. Meanwhile, the Decision Tree model exhibited higher performance with an accuracy of 89.3%. This model showed a recall of 80.9%, precision of 88.5%, and an F-measure of 83.8%. Furthermore, the RF model demonstrated results almost similar to those of the Decision Tree, with an accuracy of 89.4%, recall of 80.9%, precision of 88.6%, and an F-measure of 83.8%.

Overall, Decision Tree and Random Forest showed comparable performance with nearly identical accuracy rates. Both also exhibited similar values for recall, precision, and F-measure. However, ANN displayed lower accuracy and overall performance compared to the Decision Tree-based models. Therefore, based on this evaluation, the Decision Tree or Random Forest models might be a preferable choice for the classification task between attack and normal activities within the utilized dataset. For a clearer visual representation, please refer to Figure 4.

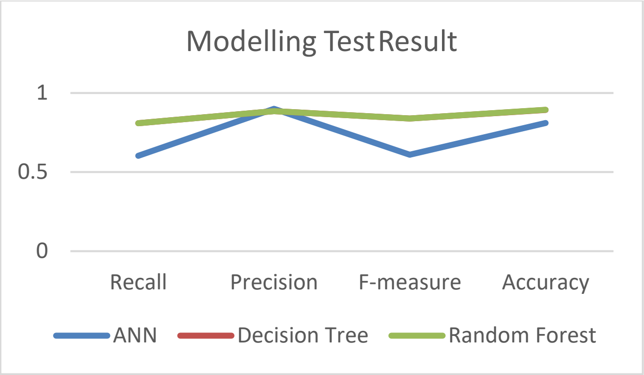

Figure 4. Visualization of Model Test Results

Based on the performance evaluation of the three tested models—ANN, RF, and Tree—it can be concluded that the RF and Decision Tree models outperformed the ANN model for the classification task between attack and normal activities within the utilized dataset. The RF and Decision Tree models exhibited nearly identical accuracy rates, approximately ranging between 89.3–89.4%, while the ANN model had an accuracy of 81%. Additionally, both Decision Tree and Random Forest showed higher values for recall, precision, and F-measure compared to the ANN model. Therefore, based on this evaluation, it can be suggested that utilizing the Decision Tree or Random Forest model might be more effective for classification in the given dataset. Although ANN holds potential for complex classifications, in this scenario, the decision tree-based models demonstrated superior and more stable performance in identifying attacks and normal activities.

Table 2. Comparison with Models in Previous Studies

Research Model	Dataset	Labeling User	Accuracy
RNN [22]	Web logs Dataset	Uncertified User	94%
LSTM [30]	HTTP Web Request dataset (Open Source)	Unknown User	78%
CatBoost [31]	multi-label SR-BH 2020 dataset (Open Source)	Unknown User	88%
Proposed Model	Server Logs Dataset	Security experts	89%

From Table 2, it can be observed that two previous studies had lower accuracy compared to the proposed model. However, one prior study by Eunancy, utilizing RNN with web logs (not server logs), achieved high accuracy. While the processed data may have had high density, there remains a significant question regarding the determination of target attributes/labels of the dataset, as its credibility was not provided. Therefore, it can be concluded that the proposed model with the generated dataset is sufficient to contribute to further research.

CONCLUSION

Based on the findings of this research, it can be concluded that combining expert labeling with the selection of the optimal classification model significantly improves the accuracy of attack detection in web application server access logs. The expert labeling process, which involves security professionals in determining the status of log entries (safe or attack), yields insightful distinctions among subtle and evolving attack patterns. Incorporating expert knowledge into this process enhances the precision of attack identification. Additionally, tailoring the selection of a classification model to the specific characteristics of server log data contributes to improved attack detection accuracy. Through a comprehensive comparison of various classification models, this study successfully identified the most suitable model capable of handling the complexity of attack patterns within log data. The involvement of multiple security experts in labeling the server log dataset, coupled with the application of validation and consistency in labeling across different datasets, serves to reduce errors and bolster confidence in the final dataset outcomes. Consequently, the integrated approach of expert labeling and the thoughtful selection of a classification model represents a progressive step in addressing evolving cyber threats, strengthening attack detection capabilities in web applications, and enhancing the reliability of information security systems. As a suggestion for future work, further exploration into more heterogeneous datasets involving multiple servers could be undertaken to train more precise models and achieve higher accuracy results.

REFERENCES

[1] C. T. Yang, Y. W. Chan, J. C. Liu, E. Kristiani, and C. H. Lai, "Cyberattacks detection and analysis in a network log system using XGBoost with ELK stack," *Soft Computing*, vol. 26, no. 11, pp. 5143–5157, Jun. 2022, doi: 10.1007/S00500-022-06954-8/METRICS.

[2] M. Landauer, M. Frank, F. Skopik, W. Hotwagner, M. Wurzenberger, and A. Rauber, "A Framework for Automatic Labeling of Log Datasets from Model-driven Testbeds for HIDS Evaluation," *SaT-CPS 2022 - Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems*, pp. 77–86, Apr. 2022, doi: 10.1145/3510547.3517924.

[3] N. Zagorodna, M. Stadnyk, B. Lypa, M. Gavrylov, and R. Kozak, "Network Attack Detection Using Machine Learning Methods," *Challenges to national defence in contemporary geopolitical situation*, vol. 2022, no. 1, pp. 55–61, Nov. 2022, doi: 10.47459/CNDCGS.2022.7.

[4] I. Riadi, R. Umar, and A. Sugandi, "Web Forensic on Container Services Using Grr Rapid Response Framework," *Scientific Journal of Informatics*, vol. 7, no. 1, pp. 33–42, Jun. 2020, doi: 10.15294/SJI.V7I1.18299.

[5] A. Thakkar and R. Lohiya, "Attack classification using feature selection techniques: a comparative study," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 1249–1266, Jan. 2021, doi: 10.1007/S12652-020-02167-9/METRICS.

[6] G. Xu *et al.*, "Real-Time Diagnosis of Configuration Errors for Software of AI Server Infrastructure," *IEEE Transactions on Dependable and Secure Computing*, no. 01, pp. 1–12, Apr. 2023, doi: 10.1109/TDSC.2023.3266007.

[7] S. Sulaimany and A. Mafakheri, "Visibility graph analysis of web server log files," *Physica A: Statistical Mechanics and its Applications*, vol. 611, p. 128448, Feb. 2023, doi: 10.1016/J.PHYSA.2023.128448.

[8] W. Wagito and L. Dison, "ANALISIS DATA AKSES SITUS BERDASAR TEKNOLOGI LOG SERVER," *Technologia : Jurnal Ilmiah*, vol. 13, no. 1, pp. 22–29, Jun. 2022, doi: 10.31602/TJI.V13I1.6113.

[9] S. Ghareeb, M. Mahyoub, and J. Mustafina, "Analysis of Feature Selection and Phishing Website Classification Using Machine Learning," *Proceedings - International Conference on Developments in eSystems Engineering, DeSE*, vol. 2023-January, pp. 178–183, 2023, doi: 10.1109/DESE58274.2023.10099697.

[10] A. Truong, S. R. Etesami, and N. Kiyavash, "Selective Labeling in Learning with Expert Advice," *Proceedings of the American Control Conference*, vol. 2021-May, pp. 2537–2542, May 2021, doi: 10.23919/ACC50511.2021.9482705.

[11] Q. Jia, G. Jin, Y. Li, X. Tang, S. Xu, and H. Ye, "Labeling Expert: A New Multi-Network Anomaly Detection Architecture Based on LNN-RLSTM," *Applied Sciences 2023, Vol. 13, Page 581*, vol. 13, no. 1, p. 581, Dec. 2022, doi: 10.3390/APP13010581.

[12] S. Lad, "Application and Data Security Patterns," *Azure Security For Critical Workloads*, pp. 111–133, 2023, doi: 10.1007/978-1-4842-8936-5_5.

[13] B. Erşahin and M. Erşahin, "Web application security," *South Florida Journal of Development*, vol. 3, no. 4, pp. 4194–4203, Jul. 2022, doi: 10.46932/sfjdv3n4-002.

[14] W. Wang, F. Dumont, N. Niu, and G. Horton, "Detecting Software Security Vulnerabilities Via Requirements Dependency Analysis," *IEEE Transactions on Software Engineering*, vol. 48, no. 05, pp. 1665–1675, May 2022, doi: 10.1109/TSE.2020.3030745.

[15] H. Dam, T. Tran, T. Pham, S. Ng, J. Grundy, and A. Ghose, "Automatic Feature Learning for Predicting Vulnerable Software Components," *IEEE Transactions on Software Engineering*, vol. 47, no. 01, pp. 67–85, Jan. 2021, doi: 10.1109/TSE.2018.2881961.

[16] B. Reddy Bhimireddy, A. Nimmagadda, H. Kurapati, L. Reddy Gogula, R. Rani Chintala, and V. Chandra Jadala, "Web Security and Web Application Security: Attacks and Prevention," *2023 9th International Conference on Advanced Computing and Communication Systems, ICACCS 2023*, pp. 2095–2099, 2023, doi: 10.1109/ICACCS57279.2023.10112741.

[17] C. Mohan and D. Dath, "Automatic Attack Detection with Machine Learning and Secure Log for Cloud Forensics," *ICISTSD 2022 - 3rd International Conference on Innovations in Science and Technology for Sustainable Development*, pp. 248–252, 2022, doi: 10.1109/ICISTSD55159.2022.10010556.

[18] S. Saleem, M. Sheeraz, M. Hanif, and U. Farooq, "Web Server Attack Detection using Machine Learning," *1st Annual International Conference on Cyber Warfare and Security, ICCWS 2020 - Proceedings*, Oct. 2020, doi: 10.1109/ICCWS48432.2020.9292393.

[19] S. Tarannum, S. M. M. Hossain, and T. Sayeed, "Cyber Security Issues: Web Attack Investigation," *Lecture Notes in Networks and Systems*, vol. 647 LNNS, pp. 1254–1269, 2023, doi: 10.1007/978-3-031-27409-1_115/COVER.

[20] A. T. Tran, T. D. Luong, X. S. Pham, and T. L. Tran, "Deep Models with Differential Privacy for Distributed Web Attack Detection," *Proceedings - International Conference on Knowledge and Systems Engineering, KSE*, vol. 2022-October, 2022, doi: 10.1109/KSE56063.2022.9953788.

[21] O. G. Awuor, "Assessment of existing cyber-attack detection models for web-based systems," *https://gjeta.com/sites/default/files/GJETA-2023-0075.pdf*, vol. 15, no. 1, pp. 070–089, Apr. 2023, doi: 10.30574/GJETA.2023.15.1.0075.

[22] J. I. Christy Eunaicy and S. Suguna, "Web attack detection using deep learning models," *Materials Today: Proceedings*, vol. 62, pp. 4806–4813, Jan. 2022, doi: 10.1016/J.MATPR.2022.03.348.

[23] C. D. D. Rupprecht, L. Fujiyoshi, S. R. McGreevy, and I. Tayasu, "Trust me? Consumer trust in expert information on food product labels," *Food and Chemical Toxicology*, vol. 137, p. 111170, Mar. 2020, doi: 10.1016/J.FCT.2020.111170.

[24] N. Fitzgerald, O. Täckström, K. Ganchev, and D. Das, "Semantic Role Labeling with Neural Network Factors," *Conference Proceedings - EMNLP 2015: Conference on Empirical Methods in Natural Language Processing*, pp. 960–970, 2015, doi: 10.18653/V1/D15-1112.

[25] M. Muller *et al.*, "Designing Ground Truth and the Social Life of Labels," pp. 1–16, May 2021, doi: 10.1145/3411764.3445402.

[26] P. Donmez, J. G. Carbonell, and J. Schneider, "Efficiently learning the accuracy of labeling sources for selective sampling," *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 259–267, 2009, doi: 10.1145/1557019.1557053.

[27] A. K. Silivery, K. R. M. Rao, and L. K. Suresh Kumar, "An Effective Deep Learning Based Multi-Class Classification of DoS and DDoS Attack Detection," *International Journal of Electrical and Computer Engineering Systems*, vol. 14, no. 4, pp. 421–431, Apr. 2023, doi: 10.32985/IJECES.14.4.6.

[28] F. Nazarudeen and S. Sundar, "Efficient DDoS Attack Detection using Machine Learning Techniques," *2022 IEEE International Power and Renewable Energy Conference, IPRECON 2022*, 2022, doi: 10.1109/IPRECON55716.2022.10059561.

[29] S. Santhosh, M. Sambath, and J. Thangakumar, "Detection of DDOS Attack using Machine Learning Models," *Proceedings of the 1st IEEE International Conference on Networking and Communications 2023, ICNWC 2023*, 2023, doi: 10.1109/ICNWC57852.2023.10127537.

[30] R. L. Alaoui and E. H. Nfaoui, "Web attacks detection using stacked generalization ensemble for LSTMs and word embedding," *Procedia Computer Science*, vol. 215, pp. 687–696, Jan. 2022, doi: 10.1016/J.PROCS.2022.12.070.

[31] T. S. Riera, J. R. B. Higuera, J. B. Higuera, J. J. M. Herraiz, and J. A. S. Montalvo, "A new multi-label dataset for Web attacks CAPEC classification using machine learning techniques," *Computers & Security*, vol. 120, p. 102788, Sep. 2022, doi: 10.1016/J.COSE.2022.102788.

[32] S. Qiu, H. Huang, W. Jiang, F. Zhang, and W. Zhou, "Defect Prediction via Tree-Based Encoding with Hybrid Granularity for Software Sustainability," *IEEE Transactions on Sustainable Computing*, no. 01, pp. 1–12, Feb. 2023, doi: 10.1109/TSUSC.2023.3248965.

[33] P. A. Bayupati, A. A. A. S. Dewi, and N. K. A. Wirdiani, "Perbandingan Metode Artificial Neural Network dan Artificial Neural Network untuk Memprediksi Jumlah Distribusi Air di PDAM Kota Denpasar," *JST (Jurnal Sains dan Teknologi)*, vol. 12, no. 2, Oct. 2023, doi: 10.23887/JSTUNDIKSHA.V12I2.47800.

[34] G. Ibarra-Vazquez, M. Soledad Ramírez-Montoya, H. Terashima, and H. Terashima terashima, "Education and Information Technologies Gender prediction based on University students' complex thinking competency: An analysis from machine learning approaches", doi: 10.1007/s10639-023-11831-4.

[35] R. Meenal, P. A. Michael, D. Pamela, and E. Rajasekaran, "Weather prediction using random forest machine learning model," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 2, pp. 1208–1215, May 2021, doi: 10.11591/IJEECS.V22.I2.PP1208-1215.

[36] L. Alfaris, R. C. Siagian, A. C. Muhammad, U. I. Nyuswantoro, N. Laeiq, and F. D. Mobo, "Classification of Spiral and Non-Spiral Galaxies using Decision Tree Analysis and Random Forest Model: A Study on the Zoo Galaxy Dataset," *Scientific Journal of Informatics*, vol. 10, no. 2, pp. 139–150, May 2023, doi: 10.15294/SJI.V10I2.44027.

[37] D. Supriyadi *et al.*, "Klasifikasi Loyalitas Pengguna Sistem E-Learning Menggunakan Net Promoter Score dan Machine Learning," *JEPIN (Jurnal Edukasi dan Penelitian Informatika)*, vol. 8, no. 1, pp. 38–43, Apr. 2022, doi: 10.26418/JP.V8I1.49300.

[38] A. M. Alfatah, R. Arifudin, and M. A. Muslim, "Implementation of Decision Tree and Dempster Shafer on Expert System for Lung Disease Diagnosis," *Scientific Journal of Informatics*, vol. 5, no. 1, p. 57, May 2018, doi: 10.15294/SJI.V5I1.13440.