Figure 11 compares DDoS attack classification performance using SVM, Random Forest, and Naïve Bayes. The XGBoost and Random Forest algorithms achieved the highest accuracy in classifying DDoS attack types. Among all methods, XGBoost proved to be the most effective in detecting different DDoS attacks.

Table VIII displays the test results obtained using a new DDoS attack dataset from www.kaggle.com. Researchers used this dataset to evaluate the model by comparing actual labels with predicted DDoS attack classifications. In the previous study [83] which discussed DDoS attacks with an ensemble learning approach with the accuracy of the model's computation results reaching 70% - 99.35% compared to our study which found a novelty in the accuracy of the combination of ensemble learning models in case of data imbalance problems using ensemble learning with a combination of PCA or undersampling with a hybrid approach that better preserves the richness of the data set. This means that the research model can perfectly distinguish between DDoS attacks and normal network traffic by correctly flagging all attacks without giving false alarms to the system. The capabilities of this model show excellence in recognizing patterns in the data.

## V. CONCLUSION

This study examines the effectiveness of the Extreme Gradient Boosting (XGBoost) algorithm in detecting Distributed Denial of Service (DDoS) attacks on the Internet of Medical Things (IoMT) network by overcoming data imbalance problems using Principal Component Analysis (PCA) and undersampling techniques. The experiment results showed that the XGBoost + PCA + Undersampling method provided classification performance with an accuracy of 99.92%. Compared to the XGBoost + PCA method, which reached 99.95%, and XGBoost + Undersampling, which obtained the best performance of 99.98%, the proposed technique was proven to be able to improve the stability of the model in the face of unbalanced data distribution. This result also proves that combining XGBoost + Undersampling DDoS cases on IoMT systems shows significant results. Thus, this combination reinforces a robust model of unbalanced data for classification in strengthening network security in IoT-based medical environments. Future research could explore adaptive ensemble strategies or deep learning integration for real-time DDoS mitigation in IoMT.

## REFERENCES


[1] A. A. Alahmadi *et al.*, 'DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions', *Electronics*, vol. 12, no. 14, p. 3103, Jul. 2023, doi: 10.3390/electronics12143103.

[2] P. Matthew *et al.*, 'A Review of the State of the Art for the Internet of Medical Things', *Sci*, vol. 7, no. 2, p. 36, Mar. 2025, doi: 10.3390/sci7020036.

[3] M. Aljebreen, H. A. Mengash, M. A. Arasi, S. S. Aljameel, A. S. Salama, and M. A. Hamza, 'Enhancing DDoS Attack Detection Using Snake Optimizer With Ensemble Learning on Internet of Things Environment', *IEEE Access*, vol. 11, pp. 104745–104753, 2023, doi: 10.1109/ACCESS.2023.3318316.

[4] J. Wang, Y. Liu, H. Feng, and National Engineering Laboratory on Interconnection Technology for Next Generation Internet, Beijing Jiaotong University, Beijing, China, 'IFACNN: efficient DDoS attack detection based on improved firefly algorithm to optimize convolutional neural networks', *MBE*, vol. 19, no. 2, pp. 1280–1303, 2021, doi: 10.3934/mbe.2022059.

[5] T. N. I. Alrumaih and M. J. F. Alenazi, 'ERINDA: A novel framework for Enhancing the Resilience of Industrial Networks against DDoS Attacks with adaptive recovery', *Alexandria Engineering Journal*, vol. 121, pp. 248–262, May 2025, doi: 10.1016/j.aej.2025.02.042.

[6] M. Ali, Y. Saleem, S. Hina, and G. A. Shah, 'DDoSViT: IoT DDoS attack detection for fortifying firmware Over-The-Air (OTA) updates using vision transformer', *Internet of Things*, vol. 30, p. 101527, Mar. 2025, doi: 10.1016/j.iot.2025.101527.

[7] F. M. Aswad, A. M. S. Ahmed, N. A. M. Alhammadi, B. A. Khalaf, and S. A. Mostafa, 'Deep learning in distributed denial-of-service attacks detection method for Internet of Things networks', *Journal of Intelligent Systems*, vol. 32, no. 1, p. 20220155, Jan. 2023, doi: 10.1515/jisys-2022-0155.

[8] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, 'DDoS in the IoT: Mirai and Other Botnets', *Computer*, vol. 50, no. 7, pp. 80–84, 2017, doi: 10.1109/MC.2017.201.

[9] D. Kopp, C. Dietzel, and O. Hohlfeld, 'DDoS Never Dies? An IXP Perspective on DDoS Amplification Attacks', Mar. 07, 2021, *arXiv*: arXiv:2103.04443. doi: 10.48550/arXiv.2103.04443.

[10] M. Ibrahim and A. Al-Wadi, 'Enhancing IoMT network security using ensemble learning-based intrusion detection systems', *Journal of Engineering Research*, p. S2307187724002906, Dec. 2024, doi: 10.1016/j.jer.2024.12.003.

[11] M. L. Hernandez-Jaimes, A. Martinez-Cruz, K. A. Ramírez-Gutiérrez, and C. Feregrino-Uribe, 'Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures', *Internet of Things*, vol. 23, p. 100887, Oct. 2023, doi: 10.1016/j.iot.2023.100887.

[12] M. A. Khatun, S. F. Memon, C. Eising, and L. L. Dhirani, 'Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation', *IEEE Access*, vol. 11, pp. 145869–145896, 2023, doi: 10.1109/ACCESS.2023.3346320.

[13] G. Sripriyanka and A. Mahendran, 'Securing IoMT: A Hybrid Model for DDoS Attack Detection and COVID-19 Classification', *IEEE Access*, vol. 12, pp. 17328–17348, 2024, doi: 10.1109/ACCESS.2024.3354034.

[14] A. H. Mohd Aman, W. H. Hassan, S. Sameen, Z. S. Attarbashi, M. Alizadeh, and L. A. Latiff, 'IoMT amid COVID-19 pandemic: Application, architecture, technology, and security', *Journal of Network and Computer Applications*, vol. 174, p. 102886, Jan. 2021, doi: 10.1016/j.jnca.2020.102886.

[15] E. S. Soegoto *et al.*, 'A systematic Literature Review of Internet of Things for Higher Education: Architecture and Implementation', *Indonesian J. Sci. Technol*, vol. 7, no. 3, pp. 511–528, Oct. 2022, doi: 10.17509/ijost.v7i3.51464.

[16] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, 'Toward a Lightweight Intrusion Detection System for the Internet of Things', *IEEE Access*, vol. 7, pp. 42450–42471, 2019, doi: 10.1109/ACCESS.2019.2907965.

[17] A. Naghib, F. S. Gharehchopogh, and A. Zamanifar, 'A comprehensive and systematic literature review on intrusion detection systems in the internet of medical things: current status, challenges, and opportunities', *Artif Intell Rev*, vol. 58, no. 4, p. 114, Jan. 2025, doi: 10.1007/s10462-024-11101-w.

[18] F. Matloob *et al.*, 'Software Defect Prediction Using Ensemble Learning: A Systematic Literature Review', *IEEE Access*, vol. 9, pp. 98754–98771, 2021, doi:

10.1109/ACCESS.2021.3095559.
[19] T. Hasegawa and K. Kondo, 'Easy Ensemble: Simple Deep Ensemble Learning for Sensor-Based Human Activity Recognition', Mar. 08, 2022, *arXiv*: arXiv:2203.04153. doi: 10.48550/arXiv.2203.04153.
[20] G. Lazrek, K. Chetioui, Y. Balboul, S. Mazer, and M. El Bekkali, 'An RFE/Ridge-ML/DL based anomaly intrusion detection approach for securing IoMT system', *Results in Engineering*, vol. 23, p. 102659, Sep. 2024, doi: 10.1016/j.rineng.2024.102659.
[21] Z. Jia *et al.*, 'Time-domain inversion of random dynamic loads on offshore platforms based on optimized ensemble learning', *Ocean Engineering*, vol. 315, p. 119822, Jan. 2025, doi: 10.1016/j.oceaneng.2024.119822.
[22] A. Y. Taha, S. Tiun, A. H. A. Rahman, M. Ayob, and A. S. Abdulameer, 'Unified Graph-Based Missing Label Propagation Method for Multilabel Text Classification', *Symmetry*, vol. 14, no. 2, p. 286, Jan. 2022, doi: 10.3390/sym14020286.
[23] Z. Alwaisi, T. Kumar, E. Harjula, and S. Soderi, 'Securing constrained IoT systems: A lightweight machine learning approach for anomaly detection and prevention', *Internet of Things*, vol. 28, p. 101398, Dec. 2024, doi: 10.1016/j.iot.2024.101398.
[24] S. Lipsa, R. K. Dash, and N. Ivković, 'An interpretable dimensional reduction technique with an explainable model for detecting attacks in Internet of Medical Things devices', *Sci Rep*, vol. 15, no. 1, p. 8718, Mar. 2025, doi: 10.1038/s41598-025-93404-8.
[25] M. Salmi, D. Atif, D. Oliva, A. Abraham, and S. Ventura, 'Handling imbalanced medical datasets: review of a decade of research', *Artif Intell Rev*, vol. 57, no. 10, p. 273, Sep. 2024, doi: 10.1007/s10462-024-10884-2.
[26] A. Hirsi *et al.*, 'Comprehensive Analysis of DDoS Anomaly Detection in Software-Defined Networks', *IEEE Access*, vol. 13, pp. 23013–23071, 2025, doi: 10.1109/ACCESS.2025.3535943.
[27] D. M. A. A. Afraji, J. Lloret, and L. Peñalver, 'Deep learning-driven defense strategies for mitigating DDoS attacks in cloud computing environments', *Cyber Security and Applications*, vol. 3, p. 100085, Dec. 2025, doi: 10.1016/j.csa.2025.100085.
[28] G. Srinivasa Rao, P. Santosh Kumar Patra, V. A. Narayana, A. Raji Reddy, G. N. V. Vibhav Reddy, and D. Eshwar, 'DDoSNet: Detection and prediction of DDoS attacks from realistic multidimensional dataset in IoT network environment', *Egyptian Informatics Journal*, vol. 27, p. 100526, Sep. 2024, doi: 10.1016/j.eij.2024.100526.
[29] A. V. Kachavimath and N. D G, 'An Efficient DDoS Attack Detection in SDN using Multi-Feature Selection and Ensemble Learning', *Procedia Computer Science*, vol. 252, pp. 241–250, 2025, doi: 10.1016/j.procs.2024.12.026.
[30] B. Sapkota, A. Ray, M. K. Yadav, B. R. Dawadi, and S. R. Joshi, 'Machine Learning-Based Attack Detection and Mitigation with Multi-Controller Placement Optimization over SDN Environment', *JCP*, vol. 5, no. 1, p. 10, Mar. 2025, doi: 10.3390/jcp5010010.
[31] C. Vairetti, J. L. Assadi, and S. Maldonado, 'Efficient Hybrid Oversampling and Intelligent Undersampling for Imbalanced Big Data Classification', Oct. 09, 2023, *arXiv*: arXiv:2310.05789. doi: 10.48550/arXiv.2310.05789.
[32] M. Ma, N. T. Nguyen, I. Atzeni, and M. Juntti, 'Analysis of Oversampling in Uplink Massive MIMO-OFDM with Low-Resolution ADCs', in *2023 IEEE 24th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Sep. 2023, pp. 626–630. doi: 10.1109/SPAWC53906.2023.10304436.
[33] F. Ashfaq, M. Wasim, M. A. Shah, A. Ahad, and I. M. Pires, 'Enhancing Security in 5G Edge Networks: Predicting Real-Time Zero Trust Attacks Using Machine Learning in SDN Environments', *Sensors*, vol. 25, no. 6, p. 1905, Mar. 2025, doi: 10.3390/s25061905.
[34] H. A. Butt, K. S. A. Harthy, M. A. Shah, M. Hussain, R. Amin, and M. U. Rehman, 'Enhanced DDoS Detection Using Advanced Machine Learning and Ensemble Techniques in Software Defined Networking', *CMC*, vol. 81, no. 2, pp. 3003–3031, 2024, doi: 10.32604/cmc.2024.057185.
[35] H. Park, A. El Azzaoui, and J. H. Park, 'AIDS-Based Cyber Threat Detection Framework for Secure Cloud-Native Microservices', *Electronics*, vol. 14, no. 2, p. 229, Jan. 2025, doi: 10.3390/electronics14020229.
[36] A. A. Alashhab *et al.*, 'Enhancing DDoS Attack Detection and Mitigation in SDN Using an Ensemble Online Machine Learning Model', *IEEE Access*, vol. 12, pp. 51630–51649, 2024, doi: 10.1109/ACCESS.2024.3384398.
[37] S. A. AlSharman, O. Al-Khaleel, and M. Al-Ayyoub, 'A Detailed Inspection of Machine Learning Based Intrusion Detection Systems for Software Defined Networks', *IoT*, vol. 5, no. 4, pp. 756–784, Nov. 2024, doi: 10.3390/iot5040034.
[38] P. Kumar, G. P. Gupta, and R. Tripathi, 'An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks', *Computer Communications*, vol. 166, pp. 110–124, Jan. 2021, doi: 10.1016/j.comcom.2020.12.003.
[39] H.-M. Chuang, F. Liu, and C.-H. Tsai, 'Early Detection of Abnormal Attacks in Software-Defined Networking Using Machine Learning Approaches', *Symmetry*, vol. 14, no. 6, p. 1178, Jun. 2022, doi: 10.3390/sym14061178.
[40] F. Khan, M. A. Jan, R. Alturki, M. D. Alshehri, S. T. Shah, and A. U. Rehman, 'A Secure Ensemble Learning-Based Fog-Cloud Approach for Cyberattack Detection in IoMT', *IEEE Trans. Ind. Inf.*, vol. 19, no. 10, pp. 10125–10132, Oct. 2023, doi: 10.1109/TII.2022.3231424.
[41] T. Alsolami, B. Alsharif, and M. Ilyas, 'Enhancing Cybersecurity in Healthcare: Evaluating Ensemble Learning Models for Intrusion Detection in the Internet of Medical Things', *Sensors*, vol. 24, no. 18, p. 5937, Sep. 2024, doi: 10.3390/s24185937.
[42] A. Al Abdulwahid, 'Detection of Middlebox-Based Attacks in Healthcare Internet of Things Using Multiple Machine Learning Models', *Computational Intelligence and Neuroscience*, vol. 2022, pp. 1–15, Nov. 2022, doi: 10.1155/2022/2037954.
[43] D. Sun *et al.*, 'Learning hierarchical face representation to enhance HCI among medical robots', *Future Generation Computer Systems*, vol. 118, pp. 180–186, May 2021, doi: 10.1016/j.future.2020.11.007.
[44] A. A. Toor, M. Usman, F. Younas, A. C. M. Fong, S. A. Khan, and S. Fong, 'Mining Massive E-Health Data Streams for IoMT Enabled Healthcare Systems', *Sensors*, vol. 20, no. 7, p. 2131, Apr. 2020, doi: 10.3390/s20072131.
[45] A. S. Tarawneh, A. B. Hassanat, G. A. Altarawneh, and A. Almuhaimeed, 'Stop Oversampling for Class Imbalance Learning: A Review', *IEEE Access*, vol. 10, pp. 47643–47660, 2022, doi: 10.1109/ACCESS.2022.3169512.
[46] A. Lazcano and M. A. Jaramillo-Morán, 'Data preprocessing techniques and neural networks for trended time series forecasting', *Applied Soft Computing*, vol. 174, p. 113063, Apr. 2025, doi: 10.1016/j.asoc.2025.113063.
[47] X. Cui *et al.*, 'Evaluation of Shelf Life Prediction for Broccoli Based on Multispectral Imaging and Multi-Feature Data Fusion', *Agronomy*, vol. 15, no. 4, p. 788, Mar. 2025, doi: 10.3390/agronomy15040788.
[48] Q. H. Nguyen *et al.*, 'Influence of Data Splitting on Performance of Machine Learning Models in Prediction of Shear Strength of Soil', *Mathematical Problems in Engineering*, vol. 2021, pp. 1–15, Feb. 2021, doi:

10.1155/2021/4832864.
[49] N. Ghaniaviyanto Ramadhan, Adiwijaya, W. Maharani, and A. Akbar Gozali, 'Chronic Diseases Prediction Using Machine Learning With Data Preprocessing Handling: A Critical Review', *IEEE Access*, vol. 12, pp. 80698–80730, 2024, doi: 10.1109/ACCESS.2024.3406748.
[50] T. A. Alghamdi and N. Javaid, 'A Survey of Preprocessing Methods Used for Analysis of Big Data Originated From Smart Grids', *IEEE Access*, vol. 10, pp. 29149–29171, 2022, doi: 10.1109/ACCESS.2022.3157941.
[51] H. Jahanshahi and M. G. Baydogan, 'nTreeClus: A tree-based sequence encoder for clustering categorical series', *Neurocomputing*, vol. 494, pp. 224–241, Jul. 2022, doi: 10.1016/j.neucom.2022.04.076.
[52] M. Jiang and H. Chen, 'Label-Guided Data Augmentation for Chinese Named Entity Recognition', *Applied Sciences*, vol. 15, no. 5, p. 2521, Feb. 2025, doi: 10.3390/app15052521.
[53] B. Deepa and K. Ramesh, 'Epileptic seizure detection using deep learning through min max scaler normalization', *ijhs*, pp. 10981–10996, May 2022, doi: 10.53730/ijhs.v6nS1.7801.
[54] F. Huang, Y. He, Y. Zhang, X. Deng, and W. Jiang, 'Controlling underestimation bias in reinforcement learning via minmax operation', *Chinese Journal of Aeronautics*, vol. 37, no. 7, pp. 406–417, Jul. 2024, doi: 10.1016/j.cja.2024.03.008.
[55] D. D. Olatinwo, A. Abu-Mahfouz, G. Hancke, and H. Myburgh, 'IoT-Enabled WBAN and Machine Learning for Speech Emotion Recognition in Patients', *Sensors*, vol. 23, no. 6, p. 2948, Mar. 2023, doi: 10.3390/s23062948.
[56] X. Tian and M. Chen, 'Descriptor selection for predicting interfacial thermal resistance by machine learning methods', *Sci Rep*, vol. 11, no. 1, p. 739, Jan. 2021, doi: 10.1038/s41598-020-80795-z.
[57] J. Areia, I. A. Bispo, L. Santos, and R. L. D. C. Costa, 'IoMT-TrafficData: Dataset and Tools for Benchmarking Intrusion Detection in Internet of Medical Things', *IEEE Access*, vol. 12, pp. 115370–115385, 2024, doi: 10.1109/ACCESS.2024.3437214.
[58] G. Team *et al.*, 'Gemini: A Family of Highly Capable Multimodal Models', Jun. 17, 2024, *arXiv*: arXiv:2312.11805. doi: 10.48550/arXiv.2312.11805.
[59] H. A. Tarish, R. Hassan, K. A. Z. Ariffin, and M. M. Jaber, 'Network security framework for Internet of medical things applications: A survey', *Journal of Intelligent Systems*, vol. 33, no. 1, p. 20230220, Apr. 2024, doi: 10.1515/jisys-2023-0220.
[60] N. A. Michael, M. A. Al Ibrahim, C. Scheibe, and N. Craigie, 'Best practices of utilizing Principal Component Analysis in chemostratigraphic studies', *Applied Geochemistry*, p. 106355, Mar. 2025, doi: 10.1016/j.apgeochem.2025.106355.
[61] T. Zhang, H. Su, C. Gong, S. Yang, and S. Bai, 'Rapid Optimal Control Law Generation: An MoE Based Method', *J. of Syst. Eng. Electron.*, vol. 36, no. 1, pp. 280–291, Feb. 2025, doi: 10.23919/JSEE.2025.000013.
[62] R. Zaheer, M. Kashif Hanif, M. Umer Sarwar, and R. Talib, 'Evaluating the Effectiveness of Dimensionality Reduction on Machine Learning Algorithms in Time Series Forecasting', *IEEE Access*, vol. 13, pp. 50493–50510, 2025, doi: 10.1109/ACCESS.2025.3551741.
[63] M. Carvalho, A. J. Pinho, and S. Brás, 'Resampling approaches to handle class imbalance: a review from a data perspective', *J Big Data*, vol. 12, no. 1, p. 71, Mar. 2025, doi: 10.1186/s40537-025-01119-4.
[64] M. S. Kraiem, F. Sánchez-Hernández, and M. N. Moreno-García, 'Selecting the Suitable Resampling Strategy for Imbalanced Data Classification Regarding Dataset Properties. An Approach Based on Association Models', *Applied Sciences*, vol. 11, no. 18, p. 8546, Sep. 2021, doi: 10.3390/app11188546.
[65] F. Naeimiasl, H. Vahidi, and N. Soheili, 'Leveraging Principal Component Analysis for Data-Driven and Objective Weight Assignment in Spatial Decision-Making Framework for Qanat-Induced Subsidence Susceptibility Assessment in Railway Networks', *IJGI*, vol. 14, no. 5, p. 195, May 2025, doi: 10.3390/ijgi14050195.
[66] T. Al-Shehari and R. A. Alsowail, 'An Insider Data Leakage Detection Using One-Hot Encoding, Synthetic Minority Oversampling and Machine Learning Techniques', *Entropy*, vol. 23, no. 10, p. 1258, Sep. 2021, doi: 10.3390/e23101258.
[67] R. Štrimaitis, S. Ramanauskaitė, and P. Stefanovič, 'Automated Selection of Time Series Forecasting Models for Financial Accounting Data: Synthetic Data Application', *Electronics*, vol. 14, no. 7, p. 1253, Mar. 2025, doi: 10.3390/electronics14071253.
[68] H. Qin, 'Maximal Information Coefficient-Based Undersampling Method for Highly-Imbalanced Learning', *IEEE Access*, vol. 13, pp. 4126–4135, 2025, doi: 10.1109/ACCESS.2025.3525475.
[69] Y.-S. Jeon and D.-J. Lim, 'PSU: Particle Stacking Undersampling Method for Highly Imbalanced Big Data', *IEEE Access*, vol. 8, pp. 131920–131927, 2020, doi: 10.1109/ACCESS.2020.3009753.
[70] N. Baisholan, J. E. Dietz, S. Gnatyuk, M. Turdalyuly, E. T. Matson, and K. Baisholanova, 'FraudX AI: An Interpretable Machine Learning Framework for Credit Card Fraud Detection on Imbalanced Datasets', *Computers*, vol. 14, no. 4, p. 120, Mar. 2025, doi: 10.3390/computers14040120.
[71] Y. Zhou, X. Song, and M. Zhou, 'Supply Chain Fraud Prediction Based On XGBoost Method', in *2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, Nanchang, China: IEEE, Mar. 2021, pp. 539–542. doi: 10.1109/ICBAIE52039.2021.9389949.
[72] T. Kosaka, S. Wandale, and K. Ichige, 'RSSI-Based Indoor Localization Using Two-Step XGBoost', *IEICE Commun. Express*, vol. 12, no. 12, pp. 647–650, Dec. 2023, doi: 10.23919/comex.2023XBL0123.
[73] A. Moore and M. Bell, 'XGBoost, A Novel Explainable AI Technique, in the Prediction of Myocardial Infarction: A UK Biobank Cohort Study'.
[74] Z. Zheng, S. Pan, H. Luo, and Z. Guo, 'Porosity prediction based on GS+GA-XGBoost', in *2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*, Exeter, United Kingdom: IEEE, Dec. 2020, pp. 1014–1020. doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom51426.2020.00153.
[75] H. E. Sadig *et al.*, 'Advanced time complexity analysis for real-time COVID-19 prediction in Saudi Arabia using LightGBM and XGBoost', *Journal of Radiation Research and Applied Sciences*, vol. 18, no. 2, p. 101364, Jun. 2025, doi: 10.1016/j.jrras.2025.101364.
[76] G. S. Kumar and B. Ankayarkanni, 'Leveraging Conv-XGBoost algorithm for perceived mental stress detection using Photoplethysmography', *Intelligence-Based Medicine*, vol. 11, p. 100209, 2025, doi: 10.1016/j.ibmed.2025.100209.
[77] I. Markoulidakis and G. Markoulidakis, 'Probabilistic Confusion Matrix: A Novel Method for Machine Learning Algorithm Generalized Performance Analysis', *Technologies*, vol. 12, no. 7, p. 113, Jul. 2024, doi: 10.3390/technologies12070113.
[78] M. Fahmy Amin, 'Confusion Matrix in Binary Classification Problems: A Step-by-Step Tutorial', *Journal of Engineering Research*, vol. 6, no. 5, pp. 0–0, Dec. 2022, doi:

10.21608/erjeng.2022.274526.
[79] K. Riehl, M. Neunteufel, and M. Hemberg, 'Hierarchical confusion matrix for classification performance evaluation', *Journal of the Royal Statistical Society Series C: Applied Statistics*, vol. 72, no. 5, pp. 1394–1412, Dec. 2023, doi: 10.1093/jrsssc/qlad057.
[80] S. Sudianto, Y. Herdiyeni, and L. B. Prasetyo, 'Classification of Sugarcane Area Using Landsat 8 and Random Forest based on Phenology Knowledge', Nov. 2023.
[81] S. Sudianto, 'Pre-trained BERT Architecture Analysis for Indonesian Question Answer Model', *JAETS*, vol. 6, no. 1, pp. 60–68, Dec. 2024, doi: 10.37385/jaets.v6i1.4746.
[82] S. Sudianto, J. A. A. Masheli, N. Nugroho, R. W. Ananda Rumpoko, and Z. Akhmad, 'Comparison of Support Vector Machines and K-Nearest Neighbor Algorithm Analysis of Spam Comments on Youtube Covid Omicron', *j. Teknik inform.*, vol. 15, no. 2, pp. 110–118, Dec. 2022, doi: 10.15408/jti.v15i2.24996.
[83] W.-W. Tay, S.-C. Chong, and L.-Y. Chong, 'DDoS Attack Detection with Machine Learning', *JIWE*, vol. 3, no. 3, pp. 190–207, Oct. 2024, doi: 10.33093/jiwe.2024.3.3.12.