Pertanika

PROCEEDINGS

PP

VOL. 1 (3) 2025

The 4th Applied Informatics International Conference

Guest Editors
Yusmadi Yah Jusoh, Rozi Nor Haizan Nor and Masrah Azrifah Azmi Murad

PERTANIKA JOURNALS

A scientific journal published by Universiti Putra Malaysia Press

Pertanika Proceedings
Pertanika Proceedings

PERTANIKA PROCEEDINGS

About the Proceedings

Overview

Pertanika Proceedings is an official proceedings published by Universiti Putra Malaysia. It is an open-access conference proceeding series that covers various research fields. The proceeding series is a quarterly periodical that considers for publication of original articles as per its scope. It publishes scientific outputs independently, neither accepting nor commissioning third party content.

Proceedings papers selected by the conference committee are subjected to thorough double-blinded peer-review process. Subsequently, accepted quality papers are submitted to *Pertanika* for rapid processing and publication in the *Pertanika* Proceedings. Upon publication on *Pertanika* platform, the research output is readily available with free and unlimited access to audience.

Recognized internationally, *Pertanika* is committed to providing high-quality services for conference papers and making scientific output widely available. You can utilise our experience and services to transform your conference publication into a globally accessible scientific work.

Scope

Pertanika Proceedings covers wide range of scope in the field of science, and social sciences and humanities. Area relevant to the scope are agricultural sciences, biological sciences, marine sciences, applied sciences and technologies, chemical sciences, earth sciences, engineering sciences, environmental sciences, information, computer and communication technologies, material sciences, physical sciences, medical and health sciences, mathematical science, architecture and habitat, consumer and family economics, education, consumer law, media and communication studies, political sciences and public policy, population studies, psychology, sociology, tourism, arts and culture, dance, language and linguistics, literature, music, philosophy and sports.

Aim

Pertanika aims to provide a fast, versatile, and cost-effective publication service for proceeding papers.

Vision

Our vision is to publish scientific output of international repute.

Mission

It is our mission to bring the highest quality research to the widest possible audience.

Quality

Pertanika aims for excellence, sustained by a responsible and professional approach to journal publishing, inclusively imposing the same approach to the proceedings publication. Publications are guaranteed within 90 working days upon documents and materials completion. We are committed in providing fast track platform for quality conference papers.

Publication Policy

Pertanika policy prohibits an author from submitting the same manuscript for concurrent consideration by two or more publications. It prohibits as well publication of any manuscript that has already been published either in whole or substantial part elsewhere.

Code of Ethics

Pertanika and Universiti Putra Malaysia take seriously the responsibility of all its publications to reflect the highest publication ethics. Thus, all involved parties in the publication scene with *Pertanika* are expected to abide by the *Pertanika*'s codes of ethics. Refer to *Pertanika*'s **Code of Ethics** for full details, available on the official website of *Pertanika*.

Pertanika

PROCEEDINGS

The 4th Applied Informatics International Conference

Vol. 1 (3) 2025

Guest Editors
Yusmadi Yah Jusoh, Rozi Nor Haizan Nor and Masrah Azrifah Azmi Murad

PERTANIKA JOURNALS

A scientific journal published by Universiti Putra Malaysia Press

Pertanika PROCEEDINGS
AN INTERNATIONAL PEER-REVIEWED JOURNAL

EDITORIAL OFFICE
JOURNAL DIVISION
Putra Science Park
1st Floor, IDEA Tower II
UPM-MTDC Technology Centre
Universiti Putra Malaysia
43400 Serdang, Selangor Malaysia

General Enquiry
Tel. No: +603 9769 1622
E-mail: pertanika.proceeding@upm.edu.my
URL: http://www.pertanika.upm.edu.my/

PUBLISHER
UPM Press
Universiti Putra Malaysia
43400 UPM, Serdang, Selangor,
Malaysia
Tel: +603 9769 8855
E-mail: dir.penerbit@upm.edu.my
URL: http://penerbit.upm.edu.my

Pertanika Proceedings
Vol. 1 (3) 2025

Contents

Preface

Universiti Putra Malaysia organized the 4th Applied Informatics International Conference (AiIC2024), themed "Leveraging Artificial Intelligence and Emerging Technologies in Applied Informatics." The conference was held at The Everly Hotel in Putrajaya from October 2nd to 3rd, 2024, and featured presentations of papers related to the conference theme.

The conference aimed to elevate research and innovation in Applied Informatics to an internationally recognized level by promoting collaborations between researchers from academia and industry. The papers presented at the conference focused on how artificial intelligence (AI) is applied within the informatics domain to analyze, interpret, and derive insights from data. These insights address specific challenges and enhance decision-making processes across various fields. The conference papers have since been transformed into scholarly articles in the Proceedings of AiIC2024. This publication aims to inspire scholars, researchers, and practitioners to explore potential research areas that can be developed further, enhancing our understanding from fundamental and practical perspectives.

We would like to take this opportunity to express our gratitude to our sponsors, the committee members, and the management of the Faculty of Computer Science and Information Technology at UPM, along with everyone involved in AiIC2024, for their unwavering support. Additionally, we want to acknowledge UPM Press and the team at Pertanika for their assistance in our academic endeavors and for facilitating the publication of the papers. Thank you.

Guest Editors
Yusmadi Yah Jusoh (Assoc. Prof. Ts. Dr.)
Rozi Nor Haizan Nor (Ts. Dr.)
Masrah Azrifah Azmi Murad (Assoc. Prof. Dr.)

PERTANIKA JOURNALS

PERTANIKA PROCEEDINGS

Journal homepage: http://www.pertanika.upm.edu.my/

A Conceptual Model of Diagnostic System for Monitoring Stingless Bee Colony Rehabilitation

Yang Lejing[1], Rozi Nor Haizan Nor[1]*, Yusmadi Yah Jusoh[1], Noreha Abdul Malik[2], Wan Nur Asiah Wan Mohd Adnan[3]

[1]Department of Software Engineering and Information Systems, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM), 43400 Serdang, Selangor, Malaysia
[2]Department of Electrical and Computer Engineering, Faculty of Engineering, International Islamic University Malaysia (IIUM), 53100 Gombak, Selangor, Malaysia
[3]Department of Plant Protection, Faculty of Agriculture, Universiti Putra Malaysia (UPM), 43400 Serdang, Selangor, Malaysia

ABSTRACT

The role of stingless bee colonies in ecosystems is crucial, especially their contribution to pollination. However, these bee colonies face multiple threats, such as disease and environmental changes, which could affect their health and numbers. Therefore, it is particularly important to monitor and maintain these colonies to support the stability of the ecosystem and the sustainable development of agriculture. To address this challenge, this paper proposes a new diagnostic system model designed to monitor and promote the rehabilitation of stingless bee colonies. Model of a diagnostic system for monitoring the stingless bee colony rehabilitation. The system uses a DHT11 sensor to monitor temperature and humidity, a load cell to track the hive's weight, and a force sensor to detect pressure or possible intrusion. Preliminary results show that the system can effectively capture key environmental parameters, providing valuable insights into the rehabilitation process. The findings provide avenues for further research and development of more robust monitoring solutions. This study's key contribution is combining advanced electronic information engineering techniques with ecological knowledge from previous literature. The proposed conceptual framework is an application of technical tools and a comprehensive approach to understanding and protecting these important ecosystem components. The findings highlight the importance of environmental factors for stingless bee rehabilitation and overall colony health. Environmental parameters such as temperature, humidity, and air quality are critical to the survival and development of bee colonies, directly affecting their reproduction, food supply, and disease transmission.

Keywords: Colony rehabilitation, diagnostic system, disease image processing, environment, machine learning, stingless bees

ARTICLE INFO

Article history:
Received: 30 April 2025
Published: 17 July 2025

DOI: https://doi.org/10.47836/pp.1.3.001

E-mail addresses:
yanglejing955@gmail.com (Yang Lejing)
rozinor@upm.edu.my (Rozi Nor Haizan Nor)
yusmadi@upm.edu.my (Yusmadi Yah Jusoh)
norehaa@iium.edu.my (Noreha Abdul Malik)
asiahwan@gmail.com (Wan Nur Asiah Wan Mohd Adnan)
* Corresponding author

INTRODUCTION

Meliponini (Apidae: Meliponini) are important pollinators in tropical and subtropical regions and contribute to agriculture and biodiversity (Jaffe et al., 2015; Toledo-Hernandez et al., 2022). They are adaptable, reproducible, and produce economically valuable products such as honey and propolis (Toledo-Hernandez et al., 2022). However, habitat loss, pesticides, climate change, and disease threaten stingless bee populations (Gilbert, 2016; Hashim et al., 2022), requiring ongoing management and protection. To monitor stingless colonies, studies have employed non-invasive methods such as analyzing honey, pollen, and propolis, using techniques such as acoustic signals, thermal imaging, Radio-Frequency Identification (RFID) tags, and others to assess population health and productivity (Anuar et al., 2020; Hrncir et al., 2019; Nunes-Silva et al., 2019). However, these methods are costly and have poor accuracy, so more economical and accurate techniques are needed. This paper proposes a stingless beehive monitoring system that combines sensors, image processing, and machine learning, aiming to provide beekeepers and researchers with immediate and accurate hive health information, promoting early intervention and management optimization. The system adopts a Model-View-Controller (MVC) architecture to efficiently process and manage data (Schneider et al., 2012).

LITERATURE REVIEW

Recent research has focused on managing and conserving bees and stingless bees. Bilik et al. (2021) developed a real-time visual diagnostic system to monitor bee colony health; Jaffe et al. (2015) explored management practices to optimize stingless bee culture in Brazil; Rosli et al. (2022) proposed a honeycomb monitoring system based on the Internet of Things (IoT). Schneider et al. (2012) used RFID to assess the impact of pesticides on bees. Ismail (2016) reviewed the challenges of beekeeping in Malaysia and recommended developing industry standards; Hadjur et al. (2022) explored the application of IoT in precision beekeeping. As bee populations decline, technological innovation offers a solution. Miskon et al. (2022) developed a stingless bee monitoring system based on LoRa (Long Range) to monitor bee colony health in real time. Zaman and Dorin (2023) proposed a hive health monitoring framework. Radaeski and Bauermann (2021) studied the effects of plant resources on bee colonies. Becher et al. (2013) proposed a system model to study the mechanism of bee colonies coping with stressors. Anuar et al. (2023) developed a Firebase-based IoT system to monitor honeycomb status; Jailis et al. (2022) built a honeycomb monitoring system with Arduino and DHT22 sensors. These technologies drive advances in stingless bee farming and contribute to sustainable development. Research has recently focused on using advanced technologies to improve hive management and bee behavior monitoring. Anuar et al. (2021) developed an integrated wireless system to monitor colony environmental changes and their effects on behavior; Aumann et al. (2021)

proposed Janus sensor to accurately identify bee activities; Braga et al. (2020) use machine learning to analyze honeycomb states and predict risks; Cecchi et al. (2020) used sensors to reveal the relationship between bee colonies and their environment. The convergence of technologies has also facilitated the development of colony monitoring systems. Cunha et al. (2001) proposed an Internet-based system to track the impact of environmental factors on bees in real time. Edmund and Rahman (2021) developed an intelligent stingless beehive monitoring system; Cota et al. (2023) designed low-cost IoT systems; Jiang et al. (2016) designed a system based on a wireless sensor network (WSN) to accurately monitor the relationship between bee activities and the environment.

FINDINGS

Conceptual Stingless Bee Colony Rehabilitation Monitoring and Diagnosis System Model

Developing a stingless colony rehabilitation monitoring system, with electronic information technology and ecological research, aims to provide beekeepers and researchers with tools to assess colony health and rehabilitation progress. Stingless bees are important native pollinators in tropical ecosystems and are critical for maintaining biodiversity and ecological services (Toledo-Hernandez et al., 2022). However, external factors such as invaders, food, climate change, and internal factors such as queen and larval health put global stingless bee populations at risk of decline (Lail, 2021; Miskon et al., 2022). Therefore, monitoring and protecting stingless bee colonies is crucial. Colony health is affected by temperature, humidity and air quality. Precise temperature and humidity control are essential for larval health and colony functioning. Hive ventilation helps manage these environmental factors to ensure colony health. Understanding the relationship between these factors and colony recovery is critical to the persistence and robustness of stingless bees. This model shows the relationship between environmental factors and the recovery of a stingless colony (Figure 1).

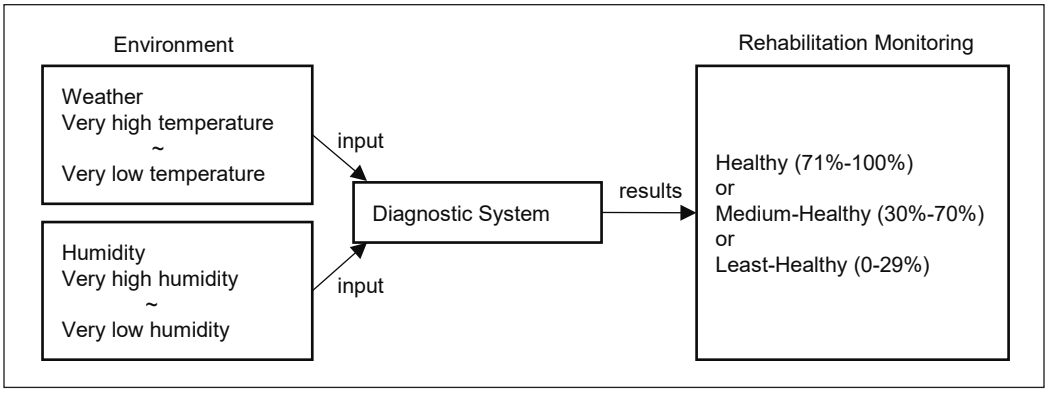

Figure 1. Diagnostic model of environmental aspects for monitoring the stingless bee colony rehabilitation

A Model View-Controller (MVC) architecture was developed to integrate user interaction, knowledge acquisition and expert decision process to enhance stingless bee monitoring and recovery. The diagnostic module allows users to intuitively judge colony health problems, such as queen bees, worker bees, temperature and humidity, and provide corresponding solutions. The system is integrated through sensor nodes, image devices, and machine learning models to process data in real time and provide feedback to beekeepers (Jaffe et al., 2015). The system combines sensors, image processing and machine learning to create a comprehensive colony monitoring and diagnosis model that helps detect anomalies on time and provides scientific evidence. This is the diagnostic model system (Figure 2).

Data preparation involves collecting and processing data on variables required for monitoring a stingless colony, such as temperature, humidity, and hive weight. It is necessary to select the appropriate sensor and data acquisition system to ensure the data's accuracy, reliability and real-time, and to store and back up the data. Hive health was assessed by the degree of pollen expansion: healthy hive pollen expansion 71%–100%, moderately healthy hive pollen expansion 30%–70%, and least healthy hive with less than 30% expansion and low activity (Ramli et al., 2021). This module shows the rehabilitation monitoring of the proposed system (Figure 3).

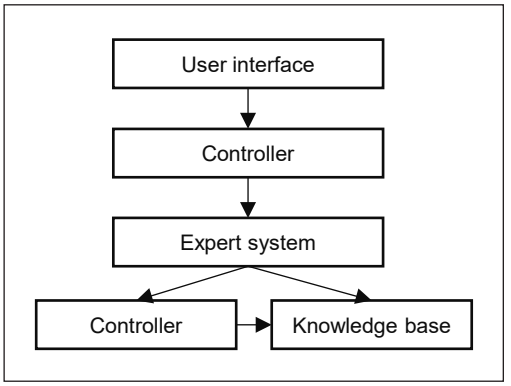

Figure 2. Diagnostic module for the proposed system

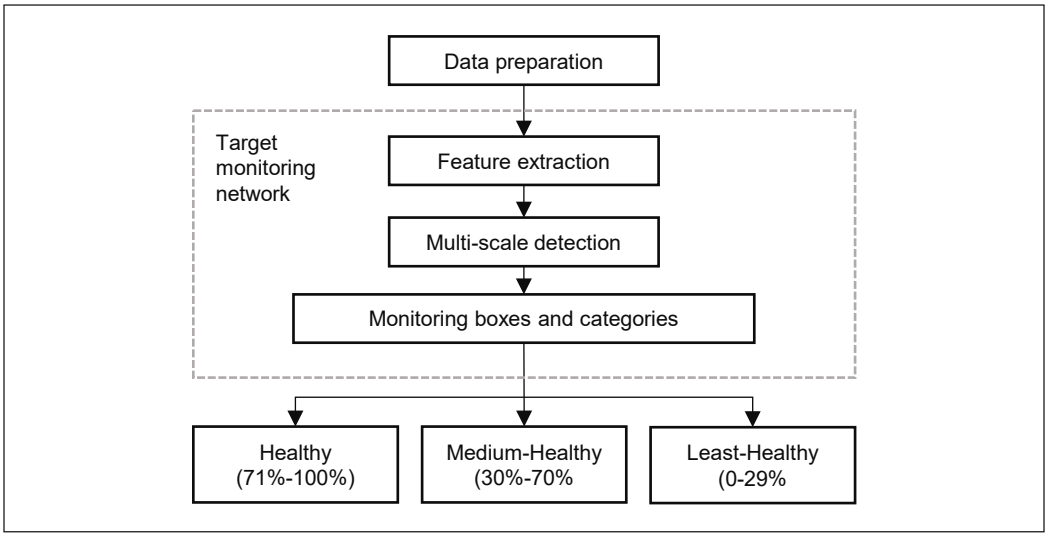

Figure 3. Rehabilitation monitoring module for the proposed system

The diagnostic system is designed to be simple and effective. It uses a DHT11 sensor to monitor the hive's temperature and humidity (Figure 4), a weighing sensor to track its weight to provide nectar and honey data, and a force sensor to detect abnormal pressure changes to indicate intrusion or structural problems.

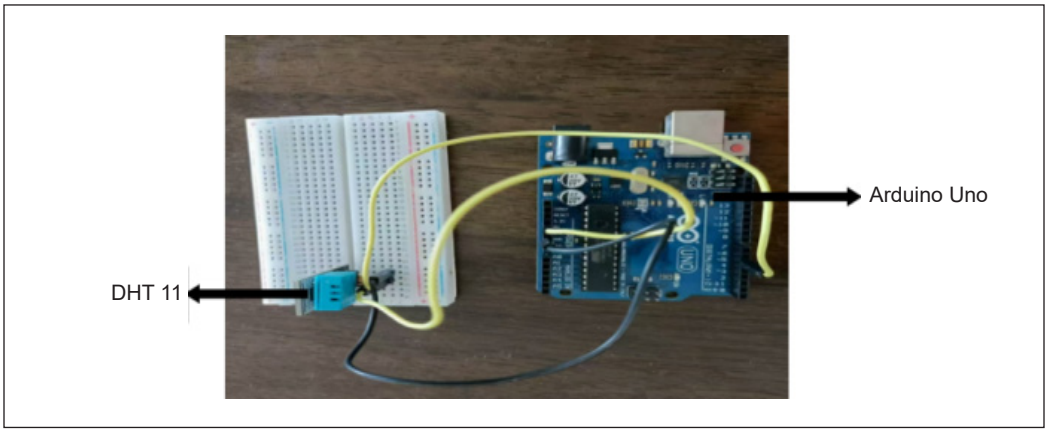

Figure 4. The DHT11 sensor circuit prototype

RESULTS

The diagnostic system effectively captures environmental parameters such as temperature, humidity, weight and pressure to provide data support for colony health. The study demonstrated the ability of the system to help beekeepers maintain sustainable bee colonies, and the future should optimize sensor integration and explore more environmental factors. The model combines sensing technology, machine learning and data evaluation to drive technological advances in beekeeping and support sustainable agriculture.

ACKNOWLEDGEMENT

We sincerely appreciate the support and provision of essential resources from Universiti Putra Malaysia (UPM) and the Faculty of Computer Science and Information Technology (UPM), which significantly contributed to the development of this project.

REFERENCES

Anuar, N. H. K., Yunus, M. A. M., Baharudin, M. A., Ibrahim, S., Sahlan, S., Hashem, M. Y. B., & Siddique, M. A. (2023). Data management system of IoT for stingless bee monitoring. *AIP Conference Proceedings 2795*(1), Article 030004. https://doi.org/10.1063/5.0121003

Anuar, N. H. K., Yunus, M. A. M., Baharudin, M. A., Ibrahim, S., & Sahlan, S. (2021). Embedded wireless stingless beehive monitoring and data management system. In *2021 IEEE International*

Conference in Power Engineering Application (ICPEA) (pp. 149-154). IEEE. https://doi.org/10.1109/ICPEA51500.2021.9417758

Anuar, N. H. K., Yunus, M. A. M., Baharudin, M. A., Ibrahim, S., & Sahlan, S. (2021). Embedded wireless stingless beehive monitoring and data management system. In *2021 IEEE International Conference in Power Engineering Application (ICPEA)* (pp. 149-154). IEEE. https://doi.org/10.1109/ICPEA51500.2021.9417758

Aumann, H. M., Aumann, M. K., & Emanetoglu, N. W. (2021). Janus: A combined radar and vibration sensor for beehive monitoring. *IEEE Sensors Letters, 5*(3), Article 1500204. https://doi.org/10.1109/LSENS.2021.3056870

Becher, M. A., Osborne, J. L., Thorbek, P., Kennedy, P. J., & Grimm, V. (2013). Towards a systems approach for understanding honeybee decline: a stocktaking and synthesis of existing models. *Journal of Applied Ecology, 50*(4), 868-880. https://doi.org/10.1111/1365-2664.12112

Bilik, S., Kratochvila, L., Ligocki, A., Bostik, O., Zemcik, T., Hybl, M., Harok, K., & Zalud, L. (2021). Visual diagnosis of the varroa destructor parasitic mite in honeybees using object detector techniques. *Sensors, 21*(8), 2764. https://doi.org/10.3390/s2108276.

Braga, A. R., Gomes, D. G., Rogers, R., Hassler, E. E., Freitas, B. M., & Cazier, J. A. (2020). A method for mining combined data from in-hive sensors, weather and apiary inspections to forecast the health status of honey bee colonies. *Computers and Electronics in Agriculture, 169*, Article 105161. https://doi.org/10.1016/j.compag.2019.105161

Cecchi, S., Spinsante, S., Terenzi, A., & Orcioni, S. (2020). A smart sensor-based measurement system for advanced bee hive monitoring. *Sensors, 20*(9), Article 2726. https://doi.org/10.3390/s20092726

Cota, D., Martins, J., Mamede, H., & Branco, F. (2023). BHiveSense: An integrated information system architecture for sustainable remote monitoring and management of apiaries based on IoT and microservices. *Journal of Open Innovation: Technology, Market, and Complexity, 9*(3), Article 100110. https://doi.org/10.1016/j.joitmc.2023.100110

Cunha, R. S. D., Saraiva, A. M., Cugnasca, C. E., Hirakawa, A. R., Imperatriz-Fonseca, V. L., & Hilário, S. D. (2001). An internet-based monitoring system for behaviour studies of stingless bees. *Proceedings of the Third European Conference of the European Federation for Information Technology in Agriculture, Food and the Environment 1*, 279-284.

Edmund, C., & Rahman, M. A. (2021). Smart stingless beehive monitoring system. In R. Alfred, H. Lida, H. Haviluddin & P. Anthony (Eds.) *Computational Science and Technology: 7th ICCST 2020* (pp. 537-549). Springer.

Gilbert, N. (2016). Global biodiversity report warns pollinators are under threat. *Nature News 2016*, Article 19456. https://doi.org/10.1038/nature.2016.19456

Hadjur, H., Ammar, D., & Lefèvre, L. (2022). Toward an intelligent and efficient beehive: A survey of precision beekeeping systems and services. *Computers and Electronics in Agriculture*, *192*, Article 106604. https://doi.org/10.1016/j.compag.2021.106604.

Hashim, S., Nassir, C. M. N. C. M., Zarim, M. H. A., Kamaruzaman, K. A., Halim, S. A., Mohamed, M., & Mustapha, M. (2022). The cerebral plasticity prospect of stingless bee honey-polyphenols supplementation

in rehabilitation of post-stroke vascular cognitive impairment. In P. Sanchetee (Ed.) *Post-Stroke Rehabilitation* (pp. 103135). IntechOpen. https://doi.org/10.5772/intechopen.103135

Hrncir, M., Maia-Silva, C., Silva Teixeira-Souza, V. H. D., & Imperatriz-Fonseca, V. L. (2019). Stingless bees and their adaptations to extreme environments. *Journal of Comparative Physiology A, 205*(3), 415-426. https://doi.org/10.1007/s00359-019-01327-3

Ismail, W. I. W. (2016). A review on beekeeping in Malaysia: History, importance, and future directions. *Journal of Sustainable Science and Management, 11*, 70–80.

Jaffe, R., Pope, N., Carvalho, A. T., Maia, U. M., Blochtein, B., Carvalho, C. A. L. D., Carvalho-Zilse, G. A., Freitas, B. M., Menezes, C., Ribeiro, M. D. F., Venturieri, G. C., & Imperatriz-Fonseca, V. L. (2015). Bees for development: Brazilian survey reveals how to optimize stingless beekeeping. *PloS one, 10*(3), Article e0121157. https://doi.org/10.1371/journal.pone.0121157.

Jailis, B. A., Kiring, A., Yew, H. T., Barukang, L., Farm, Y. Y., & Wong, F. (2022). A real-time web-based monitoring system for stingless bee farming. In *2022 IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET)* (pp. 1-5). IEEE. https://doi.org/10.1109/IICAIET55139.2022.9936841

Jiang, J. A., Wang, C. H., Chen, C. H., Liao, M. S., Su, Y. L., Chen, W. S., & Chuang, C. L. (2016). A WSN-based automatic monitoring system for the foraging behavior of honey bees and environmental factors of beehives. *Computers and Electronics in Agriculture, 123*, 304-318. https://doi.org/10.1016/j.compag.2016.03.003

Lail, M. Y. I., (2021). *Movices architecture for meliponiculture diagnostic application system development* [Unpublished master thesis]. Universiti Putra Malaysia.

Miskon, M. T., Razak, M. A. A., Jaafar, H., Hassan, N., & Mahmood, R. (2022). A lora-based testbed development for stingless bee monitoring system. *TEM Journal*, *11*(2), 712.

Nunes-Silva, P., Hrncir, M., Guimarães, J. T. F., Arruda, H., Costa, L., Pessin, G., Siqueira, J. O., Souza, P. D., & Imperatriz-Fonseca, V. L. (2019). Applications of RFID technology on the study of bees. *Insectes Sociaux, 66*(1), 15-24. https://doi.org/10.1007/s00040-018-0660-5

Radaeski, J. N., & Bauermann, S. G. (2021). Contributions to melissopalynology studies in southern Brazil: pollen analysis in the honeys from Apis mellifera, Tetragonisca angustula, Melipona quadrifasciata quadrifasciata, Scaptotrigona bipunctata, Plebeia remota and Plebeia droryana. *Palynology, 45*(3), 477-486. https://doi.org/10.1080/01916122.2020.1869113

Ramli, M. F., Harun, A., Ismail, R. C., Ndzi, D. L., Turner, J., Farook, R. S. M., & Murad, S. A. Z. (2021). Design and development of stingless beehive air pollutant monitoring system. *International Journal of Nanoelectronics & Materials, 14*(Special Issue), 265-278.

Rosli, H. A., Malik, N. A., & Ahmad, Y. A. (2022). IoT based monitoring system for stingless bees colony in IIUM. *Journal of Physics: Conference Series, 2312*(1), Article 012088. https://doi.org/10.1088/1742-6596/2312/1/012088

Schneider, C. W., Tautz, J., Grünewald, B., & Fuchs, S. (2012). RFID tracking of sublethal effects of two neonicotinoid insecticides on the foraging behavior of Apis mellifera. *PloS one, 7*(1), Article e30023. https://doi.org/10.1371/journal.pone.0030023.

Toledo-Hernandez, E., Pena-Chora, G., Hernandez-Velazquez, V. M., Lormendez, C. C., Toribio-Jimenez, J., Romero-Ramirez, Y., & Leon-Rodriguez, R. (2022). The stingless bees (Hymenoptera: Apidae: Meliponini): A review of the current threats to their survival. *Apidologie, 53*(1), Article 8. https://doi.org/10.1007/s13592-022-00913-w

Zaman, A., & Dorin, A. (2023). A framework for better sensor-based beehive health monitoring. *Computers and Electronics in Agriculture, 210*, Article 107906. https://doi.org/10.1016/j.compag.2023.107906

Pertanika Proceedings 1 (3): 9 - 12 (2025)

PERTANIKA JOURNALS

PERTANIKA PROCEEDINGS

Journal homepage: http://www.pertanika.upm.edu.my/

Cross-Project Defect Prediction Model Based on Enhanced Transfer Learning

Lian Haihua, Rodziah Atan*, Wan Nurhayati Wan Ab. Rahman and Mohd Hafeez Osman

Department of Software Engineering and Information Systems, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia

ABSTRACT

This study proposes a two-stage Cross-Project Defect Prediction (CPDP) framework to address class and feature distribution imbalance. It uses adversarial training-enhanced transfer learning to identify defective software modules. Its superiority is shown through experiments on public datasets and comparison with traditional models. The first stage involves feature extraction with two encoders and advanced preprocessing techniques. The second stage utilizes transfer learning, ensemble learning, fine-tuning, and the Synthetic Minority Oversampling Technique (SMOTE) method. Future research can expand its application and optimize the model to handle complex imbalances or incorporate other techniques to enhance predictive performance, increasing the practical potential of the CPDP model in software engineering.

Keywords: Adversarial training-GAN, cross-project software, defect patterns, loss function, prediction model, transfer learning

INTRODUCTION

In recent years, CPDP models have gained attention as manual testing in large software systems is difficult (Saeed & Saleem, 2023). They use machine learning to aid development and testing. However, traditional CPDP has low accuracy due to reliance on methods requiring identical statistical characteristics (Bala et al., 2022). Researchers have explored traditional methods to address class and feature imbalance (Wen et al., 2022; Zhao et al., 2021). This study presents a CPDP model based on adversarial training with ensemble learning, training, and fine-tuning. Contributions include enhancing transfer learning with two encoders, addressing class imbalance using SMOTE and _NNfilter, and

ARTICLE INFO

Article history:
Received: 30 April 2025
Published: 17 July 2025

DOI: https://doi.org/10.47836/pp.1.3.002

E-mail addresses:
lianhaihua59@gmail.com (Lian Haihua)
rodziah@upm.edu.my (Rodziah Atan)
wannurhayati@upm.edu.my (Wan Nurhayati Wan Ab. Rahman)
mohdhafeez@upm.edu.my (Mohd Hafeez Osman)
* Corresponding author

conducting experiments on public datasets to compare with traditional methods (Khleel & Nehéz, 2023; Szeghalmy & Fazekas, 2023).

PROBLEM STATEMENT

When addressing some problem of class imbalance, CPDP models struggle to adapt, potentially impacting model generalization performance due to the differences in scale, programming languages, and structural complexity among software projects (Govinda et al., 2023; Tang et al., 2021; Hu & Zhu, 2023). The first problem with this research is that the imbalance in the distribution of defect and non-defect samples affects the performance of CPDP models (class imbalance) (Qiao et al., 2020).

Different software projects may have different concerns, resulting in a large difference in the distribution of project features (feature distribution imbalance). For example, projects in the financial industry prioritize data security, performance and response time, while projects in the e-commerce sector focus on interface design and order processing. CPDP model performance and generalization ability might be decreased when faced with feature distribution imbalance (Hu & Zhu, 2023; Saeed & Saleem, 2023).

RESEARCH QUESTIONS

The purpose of this research is to answer the research questions as follows:

1. How can we classify class imbalance between the source and target projects in CPDP models?
2. How can feature distribution imbalance mitigation between the source project and the target project be designed in CPDP models?
3. What can the CPDP models help with risk management and decision making?

CONCLUSION

When comparing the experimental results of our research method and traditional machine learning models (Logistic Regression, SVM, Decision Tree) for defect prediction on the AEEEM dataset (EQ, ML, PDE, LC, JDT), we used the average results of different models on the AEEEM dataset. As shown in Table 1, the evaluated metrics include Accuracy, AUC

Table 1
From the comparative experimental average results

Method	Accuracy	AUC	F1 Score	Precision	Recall
SVM	0.36	0.37	0.17	0.33	0.32
Logistic regression	0.35	0.36	0.38	0.32	0.34
Decision Tree	0.43	0.43	0.48	0.42	0.35
Research	0.63	0.61	0.52	0.57	0.50

(Area Under the Curve), F1 Score, Precision, and Recall. From the average results, our proposed method achieved an Accuracy of 0.63, an AUC of 0.61, an F1 Score of 0.52, a Precision of 0.57, and a Recall of 0.50.

From the comparative experimental average results on the AEEEM dataset, it can be observed that my proposed method achieves higher predictive accuracy in cross-project defect prediction tasks compared to the three traditional methods.

The visualization results, shown in Figure 1, show that the designed method has achieved good results in cross-project defect prediction tasks. Specifically, a high recall rate indicates that actual defects can be effectively identified.

$$Recall = \frac{TP}{TP+FN} = \frac{115}{115+8} = 0.935$$

As shown in Figure 2 the ROC curve is closer to the upper left corner and the area under the precision-recall curve is larger, it indicates to a certain extent that the model has better ability to handle class imbalance and feature imbalance problems in cross-project defect prediction.

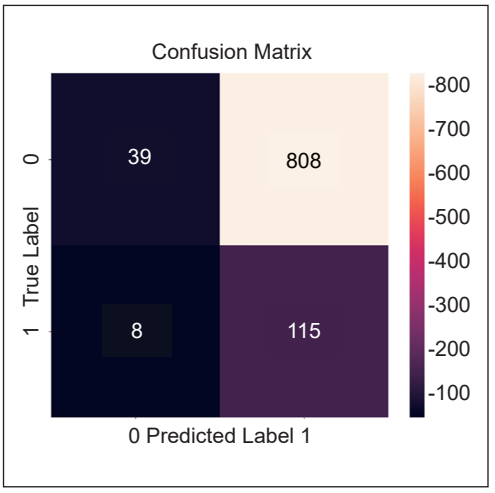

Figure 1. Result for EQ target item predicted label

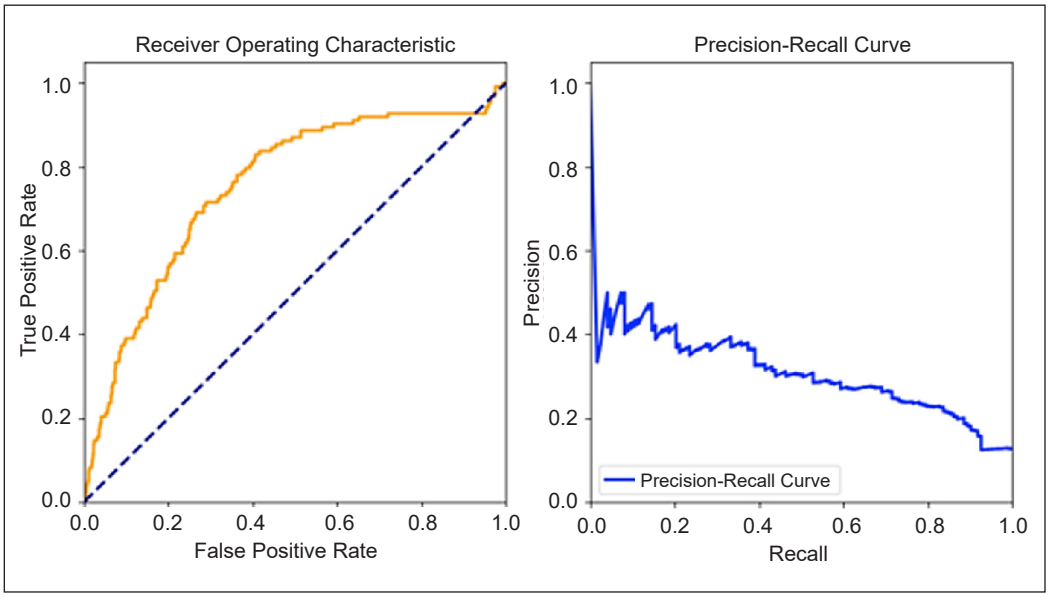

Figure 2. Result for EQ target item false positive rate and recall

ACKNOWLEDEMENT

This research owes much to many. The author is deeply grateful to Dr. Rodziah Atan for guidance, patience, and expertise. Thanks also to Dr. Wan Nurhayati Wan Ab. Rahman and Dr. Mohd Hafeez Osman for their support. The reviewers' and editors' comments improved the paper. Their encouragement kept me motivated throughout this challenging research.

REFERENCES

Bala, Y. Z., Samat, P. A., Sharif, K. Y., & Manshor, N. (2022). Improving cross-project software defect prediction method through transformation and feature selection approach. *IEEE Access*, *11*, 2318-2326. https://doi.org/10.1109/ACCESS.2022.3231456

Govinda, N. N., Lohith, R., Jha, R. K., & Gururaj, H. L. (2023). Cross-project fault prediction using artificial intelligence. *International Journal of Bioinformatics and Intelligent Computing*, *2*(1), 73-81. https://doi.org/10.61797/ijbic.v2i1.204

Hu, Z., & Zhu, Y. (2023). Cross - project defect prediction method based on genetic algorithm feature selection. *Engineering Reports*, *5*(12), Article e12670. https://doi.org/10.1002/eng2.12670

Khleel, N. A. A., & Nehéz, K. (2023). A novel approach for software defect prediction using CNN and GRU based on SMOTE Tomek method. *Journal of Intelligent Information Systems*, *60*(3), 673 - 707. https://doi.org/10.1007/s10844-023-00793-1

Qiao, L., Li, X., Umer, Q., & Guo, P. (2020). Deep learning based software defect prediction. *Neurocomputing*, *385*, 100-110. https://doi.org/10.1016/j.neucom.2019.11.067

Saeed, M. S., & Saleem, M. (2023). Cross project software defect prediction using machine learning: A review. *International Journal of Computational and Innovative Sciences*, *2*(3), 35-52.

Szeghalmy, S., & Fazekas, A. (2023). A comparative study of the use of stratified cross-validation and distribution-balanced stratified cross-validation in imbalanced learning. *Sensors, 23*(4), Article 2333. https://doi.org/10.3390/s23042333

Tang, S., Huang, S., Zheng, C., Liu, E., Zong, C., & Ding, Y. (2021). A novel cross-project software defect prediction algorithm based on transfer learning. *Tsinghua Science and Technology*, *27*(1), 41-57. https://doi.org/10.26599/TST.2020.9010040

Wen, W., Shen, C., Lu, X., Li, Z., Wang, H., Zhang, R., & Zhu, N. (2022). Cross-project software defect prediction based on class code similarity. *IEEE Access*, *10*, 105485-105495. https://doi.org/10.1109/ACCESS.2022.3211401

Zhao, Y., Zhu, Y., Yu, Q., & Chen, X. (2021). Cross-project defect prediction method based on manifold feature transformation. *Future Internet*, *13*(8), Article 216. https://doi.org/10.3390/fi13080216

Pertanika Proceedings 1 (3): 13 - 16 (2025)

PERTANIKA JOURNALS

PERTANIKA PROCEEDINGS

Journal homepage: http://www.pertanika.upm.edu.my/

Design of a Wearable Membership ID for the Fitness Center

Anugrah Adiwilaga*, Deden Pradeka, Devi Aprianti Rimadhani Agustini, Rangga Ali Mustofa, Salsabila Nida Azzahra, Ghalib Andhika Zulkhi, Aidha Salsa Billa and Mega Syarika Musharofa

Department of Computer Engineering, UPI Regional Campus Cibiru, Bandung 40625, Indonesia

ABSTRACT

The development of technology has brought major changes in aspects of life, including in the field of sports and fitness. Internet of Things (IoT) technology can improve efficiency and experience for users. Many fitness centers in Indonesia have several problems, such as fitness managers having difficulty distinguishing which member still has active memberships and which have expired ones while they are accessing the gym. The problems occur due to still adopting a manual system in terms of managing membership, granting access rights, and supervision. Therefore, this study designs and develops an integrated system that has a wearable membership ID using an nRF24 transceiver and an IoT-based Master Device to overcome these problems. The results of this work show a fully developed system that allows online registration, solid data management, seamless access granting, and real-time user safety monitoring. The performance of the system has 100% accuracy around 65 meters of Line of Sight (LOS) coverage in distinguishing between active and expired membership for access granting, which is good for improving the quality of service and the overall member experience in the future application.

Keywords: Fitness center, Internet of Things, monitoring, nRF24, wearable device

ARTICLE INFO

Article history:
Received: 30 April 2025
Published: 17 July 2025

DOI: https://doi.org/10.47836/pp.1.3.003

E-mail addresses:
anugrah.adiwilaga@upi.edu (Anugrah Adiwilaga)
dedenpradeka@upi.edu (Deden Pradeka)
deviaprianti@upi.edu (Devi Aprianti Rimadhani Agustini)
ranggaalimustofa@upi.edu (Rangga Ali Mustofa)
salsabilanida@upi.edu (Salsabila Nida Azzahra)
ghalib28@upi.edu (Ghalib Andhika Zulkhi)
aidhasalsabilla@upi.edu (Aidha Salsa Billa)
megasyarika@upi.edu (Mega Syarika Musharofa)
* Corresponding author

INTRODUCTION

The Internet of Things (IoT) has revolutionized various industries, including fitness and health, by enabling real-time data collection, analysis, and automation (Syaeh & Satino, 2024). IoT devices facilitate communication and data exchange, becoming integral to modern lifestyles, particularly fitness (Zohari et al., 2024). However, many fitness centers, like Natama's, still rely on manual systems for

e-ISSN: 3083-9475

member registration and payment, leading to inefficiencies in managing member data, such as difficulty tracking active or inactive members (Faizal, 2019).

Manual systems are prone to errors, including data loss or corruption, which can impact business operations (Liliana et al., 2021). Despite some advancements, such as the use of website-based information systems (Ridwan & Halim, 2024), integration and synchronization with other tools remain challenges. Moreover, obtaining real-time data on visitor numbers, active members, and sales is crucial for strategic decision-making (Ramadhana et al., 2021). To address these issues, a Membership and Monitoring System for Fitness Centers was developed, offering online registration and monitoring tools to streamline member management and improve operational efficiency (Kurniawan et al., 2024).

PROBLEM STATEMENT

Fitness centers, like Natama's, struggle with manual membership management, including difficulty tracking active members and limited real-time data access. These error-prone, time-consuming systems lead to data loss and operational inefficiencies. Therefore, an automated IoT-based system is needed to streamline membership management, track activity, and enhance communication and efficiency.

RESEARCH QUESTIONS

How effective is the wearable device in communicating with the master device, and what is the success rate of verifying membership data and granting access, considering different ranges and orientations?

The wearable device communicates effectively with the master device up to 65 meters (80% success rate), verifying membership data with 100% accuracy. Communication remains stable at shorter distances (30 meters) and various orientations, but drops beyond 70 meters (Tables 1–2).

Table 1
Master device coverage measurement result at 0°

Range (m)	Testing Count and Success Rate		
	Scan (Times)	Found (times)	Success Rate (%)
30	20	20	100
68.3[a]	20	16	80
70	20	0	0

*Special range sampling to see coverage limit with a success rate above 80%

Table 2
Master device coverage measurement result at 90°

Range (m)	Testing Count and Success Rate		
	Scan (Times)	Found (times)	Success Rate (%)
30	20	20	100
65.6[b]	20	17	85
70	20	0	0

*Special range sampling to see coverage limit with a success rate above 80%

CONCLUSION

The IoT-based Membership and Monitoring System improves fitness center membership management by automating the process. The wearable device reliably communicates with the master device up to 65 meters, with 100% success verifying membership data. Communication quality declines beyond 70 meters. The web server efficiently manages user data, enhancing operational efficiency and membership tracking accuracy. This system significantly improves traditional manual processes.

ACKNOWLEDGEMENT

The authors thank Universitas Pendidikan Indonesia for supporting us with the facility. This research is funded by the RKAT LPPM UPI for the 2024 Fiscal Year.

REFERENCES

Faizal, R. (2019). *Sistem Informasi Pelayanan Membership Berbasis Website Di CItra Fitness* [Website Based Membership Service Information System at Citra Fitness] [Unpublished bachelor's thesis]. Universitas Komputer Indonesia.

Kurniawan, A., Sholva, Y., & Nyoto, R. D. (2022). Aplikasi pencarian lokasi fitness beserta layanan jasa personal trainer di Kota Pontianak menggunakan metode location based service [Fitness Location Search Application and Personal Trainer Services in Pontianak City Using Location Based Service Method]. *JURISTI Jurnal Riset Sains dan Teknologi Informatika*, *1*(1), 43-50.

Liliana, D. Y., Kom, M., Andryani, N. A. C., Priandana, K., & Fitriyah, H. (2021). *Buku Literasi Informasi: Women Against Disruptive Information on Covid-19 Pandemic in Indonesia*. Cempluk Aksara.

Ramadhana, R., Pradana, F., & Arwan, A. (2021). Pengembangan sistem informasi manajemen pengelolaan member fitness dan kebutuhan nutrisi member serta pemantauan perkembangan usaha berbasis website (Studi kasus: Executive gym, Kota Cilegon) [Development of a Management Information System for Managing Fitness Members and Member Nutrition Needs and Monitoring Business Development Based on a Website (Case Study: Executive Gym, Cilegon City)]. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, *5*(12), 5449-5457.

Ridwan, M., & Halim, Z. (2023). Perancangan sistem informasi fasilitas fitness gym berbasis website menggunakan codeigniter [Design of Website-Based Gym Fitness Facility Information System Using Codeigniter]. *KLIK: Kajian Ilmiah Informatika dan Komputer*, *4*(1), 601-609. https://doi.org/10.30865/klik.v4i1.1039

Syaeh, M. T., & Satino, S. (2024). Harmoni hukum dan bisnis: Antisipasi tantangan kepatuhan dan inovasi dalam lingkungan bisnis merata-tertata berbasis e-commerce tokopedia dalam internet of things (IoT) melalui gagasan 6.0 [Harmony of Law and Business: Anticipating Compliance and Innovation Challenges in a Uniformly Organized Business Environment Based on Tokopedia's E-commerce in the Internet of Things (IoT) Through Idea 6.0]. *Innovative: Journal Of Social Science Research*, *4*(1), 957-970. https://doi.org/10.31004/innovative.v4i1.7780

Zohari, M. H., Azman, A. M., Mokhtar, M. H., Zainal, M. S., & Hussain, L. I. (2024). Bus monitoring system based on internet of things. *Journal of Advanced Industrial Technology and Application*, *5*(1), 37-44.

Pertanika Proceedings 1 (3): 17 - 21 (2025)

PERTANIKA JOURNALS

PERTANIKA PROCEEDINGS

Journal homepage: http://www.pertanika.upm.edu.my/

Development of Smart Class Attendance System: Integration of Face Recognition and Cryptography for Web-Based Data Security

Deden Pradeka*, Anugrah Adiwilaga and Devi Aprianti Rimadhani Agustini

Department of Computer Engineering, UPI Regional Campus Cibiru, Bandung 40625, Indonesia

ABSTRACT

This study develops a web-based attendance system using face recognition and cryptography to enhance data security, tailored for smart class environments. The system records attendance automatically, encrypts data for security, and integrates with Moodle for both online and offline use. It is built using Moodle as the LMS and Laravel for face recognition and encryption. The system's performance is tested under various conditions, demonstrating high accuracy in face recognition and effective data encryption. The findings suggest the system improves attendance recording efficiency and security, laying a foundation for future developments in data security using face recognition and cryptography.

Keywords: Attendance system, cryptography, data security, face recognition, Moodle, smart class, web-based

INTRODUCTION

The integration of information and communication technology has revolutionized student attendance management. Traditional systems using signatures or cards are inefficient and vulnerable to manipulation. Therefore, a more advanced and secure system is needed. Face recognition, combined with cryptography, enhances data security, ensuring confidentiality and integrity.

Integrating these technologies into Moodle, a popular LMS, supports automated attendance recording, improving efficiency. Research supports these advancements. Vyas and Rajbala (2021) highlight improvements in attendance management with automated systems. Shah et al. (2021) demonstrate cryptography's effectiveness in protecting sensitive data. Agrawal et al. (2020) suggest that deep learning enhances face recognition accuracy and efficiency. Sunaryono et al. (2021) find Android-based face recognition

ARTICLE INFO

Article history:
Received: 30 April 2025
Published: 17 July 2025

DOI: https://doi.org/10.47836/pp.1.3.004

E-mail addresses:
dedenpradeka@upi.edu (Deden Pradeka)
anugrah.adiwilaga@upi.edu (Anugrah Adiwilaga)
deviaprianti@upi.edu (Devi Aprianti Rimadhani Agustini)
* Corresponding author

systems effective. Mansoora et al. (2021) emphasize the functionality and efficiency of these methods in attendance management.

Developing a smart class attendance system integrating face recognition and cryptography can significantly improve attendance management and data security in educational environments.

PROBLEM STATEMENT

Traditional attendance systems are inefficient and prone to manipulation. This study develops a secure web-based attendance system using facial recognition and cryptography to improve accuracy and data security.

RESEARCH QUESTIONS

What is the accuracy of the facial recognition module in identifying student faces under varying conditions? The results indicate a facial recognition accuracy of 95% under ideal conditions and around 90% in low lighting and suboptimal angles, as shown in Figure 1.

How effective is the cryptography module in securing attendance data? The results of data encryption and decryption tests, shown in Table 1, demonstrate successful data integrity and confidentiality using the Advanced Encryption Standard (AES) method.

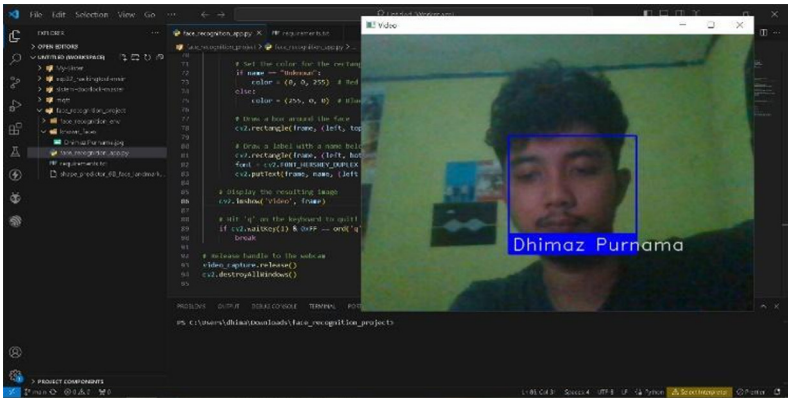

Figure 1. Result of face recognition

Table 1
Result of encrypted image

No	Image	Encrypt
1	 640 × 480	/9j/4AAQSkZJRgABAQAAAQABAAD/2wBDAAMCAgICAg……

How well does the attendance system integrate with Moodle as a Learning Management System (LMS)? Integration testing results confirm that the attendance system successfully synchronizes attendance data with Moodle, enabling efficient access for teachers and administrators. This is illustrated in Figure 2 (Teacher Dashboard Integration), highlighting its functionality.

What security measures are in place to protect transmitted data? Figure 3 illustrates the system security testing conducted with Wireshark, confirming that all transmitted data is properly encrypted to protect against unauthorized access.

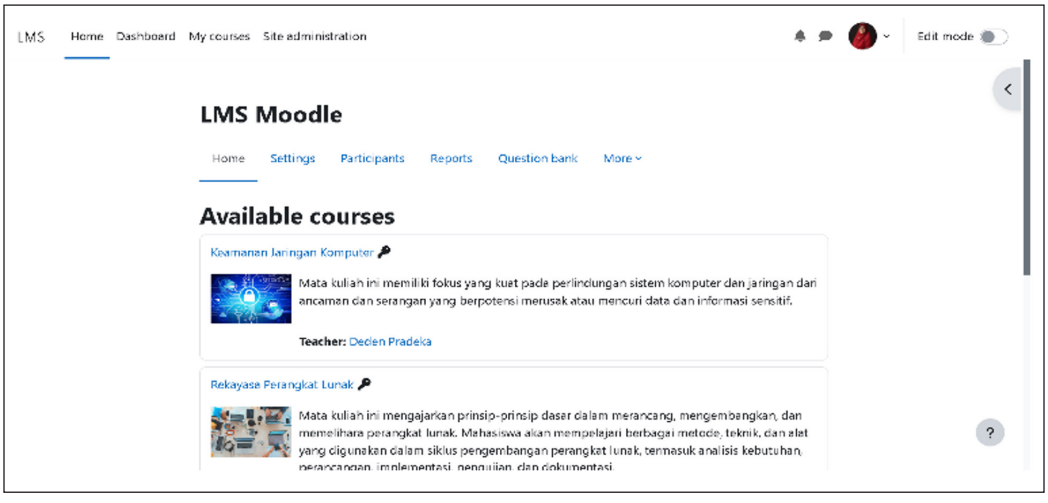

Figure 2. Dashboard teacher

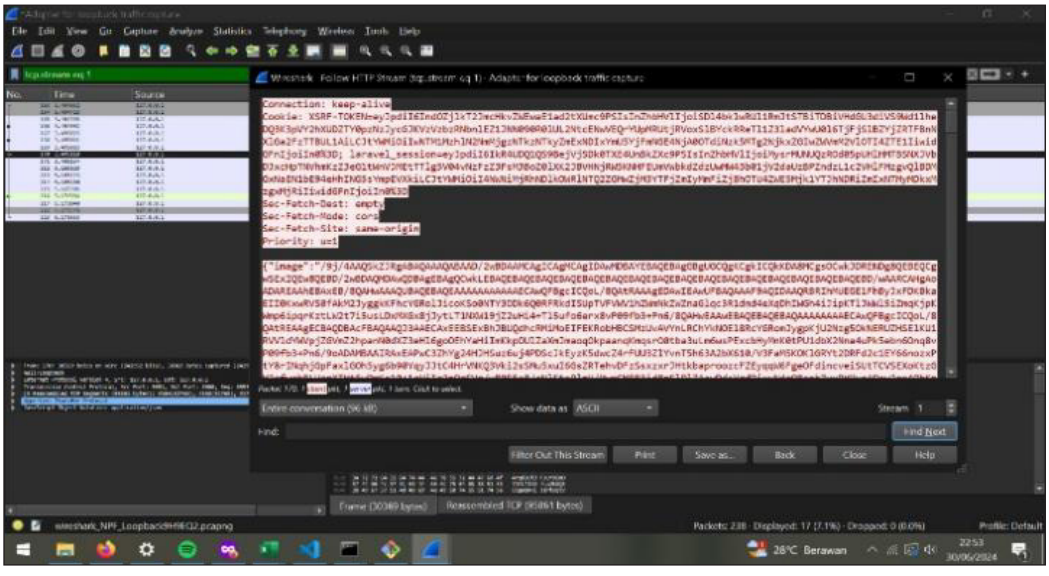

Figure 3. System security testing uses Wireshark

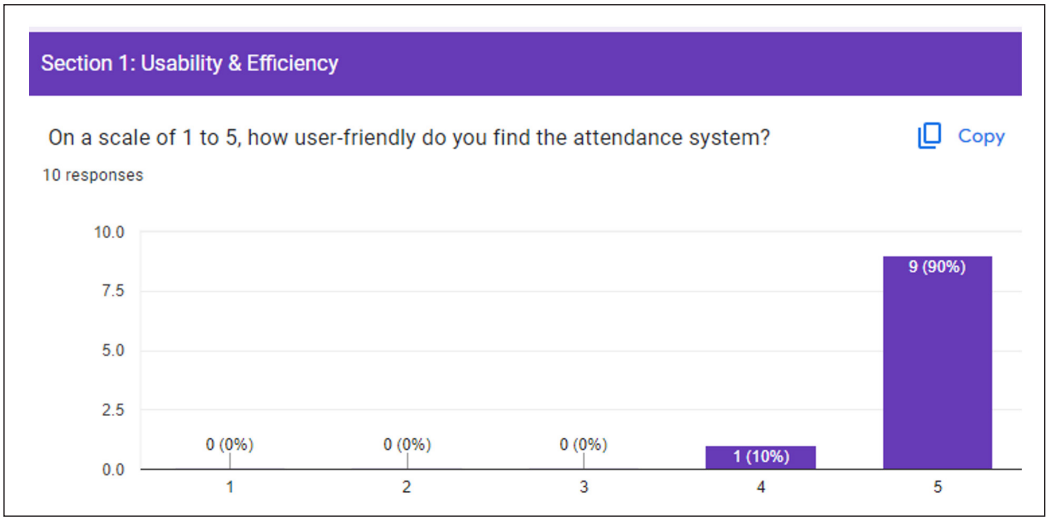

Figure 4. The respondents' feedback indicates how user-friendly the system is perceived to be

What feedback do users provide regarding the usability and impact of the attendance system? User feedback, as shown in Figure 4, indicates a general perception of the system as user-friendly and effective in improving the attendance recording process.

CONCLUSION

This research developed a web-based attendance system using facial recognition and AES encryption, achieving up to 95% accuracy and seamless integration with Moodle LMS for efficient data management. It proved secure, reliable, and user-friendly, with plans for further enhancements based on feedback.

ACKNOWLEDGEMENT

The authors thank Universitas Pendidikan Indonesia for supporting and funding this research.

REFERENCES

Agrawal, A., Garg, M., Prakash, S., Joshi, P., & Srivastava, A. M. (2020). Hand down, face up: innovative mobile attendance system using face recognition deep learning. In B. Chaudhuri, M. Nakagawa, P. Khanna & S. Kumar. (Eds.) *Proceedings of 3rd International Conference on Computer Vision and Image Processing. Advances in Intelligent Systems and Computing* (pp. 363-375). Springer. https://doi.org/10.1007/978-981-32-9291-8_29

Mansoora, S., Sadineni, G., & Kauser, S. H. (2021). Attendance management system using face recognition method. *Journal of Physics: Conference Series. 2089*(1), Article 012078. https://doi.org/10.1088/1742-6596/2089/1/012078.

Shah, K., Bhandare, D., Bhirud, S. (2021). Face recognition-based automated attendance system. In D. Gupta, A. Khanna, S. Bhattacharyya, A. E. Hassanien, S. Anand & A. Jaiswal (Eds.) *International Conference on Innovative Computing and Communications. Advances in Intelligent Systems and Computing* (pp. 945-952). Springer. https://doi.org/10.1007/978-981-15-5113-0_79

Sunaryono, D., Siswantoro, J., & Anggoro, R. (2021). An android based course attendance system using face recognition. *Journal of King Saud University-Computer and Information Sciences, 33*(3), 304-312. https://doi.org/10.1016/j.jksuci.2019.01.006

Vyas, A., & Rajbala, T. *(2020).* Face recognition-based automated attendance system. *International Journal of Recent Innovation Trends in Computing and Communication, 1*, 945–952.

Pertanika Proceedings 1 (3): 23 -25 (2025)

PERTANIKA JOURNALS

PERTANIKA PROCEEDINGS

Journal homepage: http://www.pertanika.upm.edu.my/

Active Learning Pattern Among Vocational Students: A Sequential Analysis

Eddy Azhar Jalani*, Muhd Khaizer Omar and Thinagaran Perumal

Faculty of Educational Studies, Universiti Putra Malaysia, Serdang 43400, Malaysia
Faculty of Computer Science And Information Technology, Universiti Putra Malaysia, Serdang 43400, Malaysia

ABSTRACT

This study explores the active learning patterns of vocational students in practical activities using topics related to the Internet of Things (IoT). Conducted as a case study, the research employs a combination of content analysis and sequential analysis. Active learning is implemented by assigning students practical tasks to build control systems using IoT technology. A coding scheme, defined with phrases to categorize data segments according to the studied themes, serves as a reference for evaluators to interpret students' actions and skill development during IoT-based practical tasks. The Generalized Sequential Querier (GSEQ) software is used to analyse sequential data by interpreting significant z-score values.

Keywords: Active learning, Internet of Things, practical lab activity, sequential analysis

INTRODUCTION

The emergence of the Internet of Things (IoT) has revolutionized various industries, necessitating the integration of IoT curricula into technical and vocational education and training. The practical nature of learning IoT demands hands-on experience, which is difficult to convey through traditional teaching methods. TVET instructors are struggling to adapt to the rapid technological changes brought about by the 4.0 industrial revolution, including the integration of IoT technology (Tshong & Yasin, 2023). UNESCO Education 2030 framework recognizes three principles to ensure quality education among the masses: inclusiveness, quality education, and lifelong learning. Several techniques from active learning (AL) are included in blended learning (BL), and by emphasizing student-centred learning in a far more real-world setting, these tactics enable more successful and captivating learning opportunities (Kumar et al., 2024).

ARTICLE INFO

Article history:
Received: 30 April 2025
Published: 17 July 2025

DOI: https://doi.org/10.47836/pp.1.3.005

E-mail addresses:
gs61949@student.upm.edu.my (Eddy Azhar)
khaizer@upm.edu.my (Muhd Khaizer Omar)
thinagaran@upm.edu.my (Thinagaran Perumal)
* Corresponding author

e-ISSN: 3083-9475

The construction of skills by students will be investigated in this study. Once their skill construction behaviours have been identified, a more thorough investigation will be conducted to see how they have advanced in the process and what strategies they have employed. Therefore, the goals of the research are to investigate students' active learning patterns when constructing skills in practical activities based on IoT, to identify students' strategies when constructing skills in practical activities based on IoT, and to identify the transition state of skill constructing strategies in practical activities based on IoT.

PROBLEM STATEMENT

Practical learning at the Malaysian Vocational College is now run guided by a set of practical sheets containing steps of work that have been set by the lecture to achieve learning objectives. This situation makes students only able to build skills at a low level and have limitations in exploring the practical activities they want to carry out.

RESEARCH QUESTION

Acceptance of students to this new technology raises several questions: (1) What are the active learning patterns of students that construct skills in practical activities based on the IoT? (2) What are students' strategies when constructing skills in practical activities based on the IoT? and (3) What is the transition state of skill construction strategies in practical activities based on the IoT?

This study employed the content analysis technique to investigate students' skills construction behaviours in doing practical activities based on IoT by analysing the report scripts written by the students. Based on a coding scheme, content analysis is applied to the report scripts students write for practical activities based on IoT. The coding scheme-based characterization, this study used a unit of meaning for objectivity.

For the purpose of reliability, the two raters have coded 381 messages in 3 continuous coding sessions. Table 1 shows the percentages of reliability agreement between them.

The total number of codes from 28 respondents is 340 after going through the evaluation process by two appointed raters (Table 2).

Table 1
Percentages of reliability agreement between the raters

Total code	Code gives the unit of meaning	Code agreement	Reliability percentage %
381	361	340	94

Table 2
Number of codes generated for respondents who successfully and unsuccessfully built an IoT system

Respondents	Total code	Code percentages %
Successfully built an IoT system	229	60.7
Unsuccessfully built an IoT system	111	39.3

CONCLUSION

Conclusively, this study is exploring the active learning pattern of students doing practical activities based on the IoT. The Generalized Sequential Querier (GSEQ) software is used to analyse sequential data by interpreting significant z-score values. After data analysis is done, students' skills construction can be revealed through the learning patterns and transition state diagrams that depict the initiation and follow-up strategies of students to construct skills while doing practical activities based on the IoT.

ACKNOWLEDGEMENT

The authors thank Universiti Putra Malaysia (UPM) and the Ministry of Education (MoE) Malaysia, specifically Kuala Klawang Vocational College, for their support in making this project possible. This work was supported by the Research University Grant (GP-IPS/2022/9735400) initiated by UPM and MoE as a scholarship.

REFERENCES

Kumar, A., Malhotra, S., Dias, I., & Lee, K. (2024). Active blended learning model for teaching iot application development course: Case study. *Journal of Engineering Education Transformations*, 425-431. https://doi.org/10.16920/jeet/2024/v37is2/24070

Tshong, P. K., & Yasin, R. M. (2023). TVET educational learning strategies and thier impact on student: A systematic literature review. *International Journal of Academic Research in Psychology*, 1790-1813. http://dx.doi.org/10.6007/IJARBSS/v13-i11/19558

UNESCO. (2021). UNESCO Strategy for TVET (2022-2029). *United Nations Educational, Scientific and Cultural Organization*.

Pertanika Proceedings 1 (3): 27 - 30 (2025)

PERTANIKA JOURNALS

PERTANIKA PROCEEDINGS

Journal homepage: http://www.pertanika.upm.edu.my/

Affective Intervention Based on Learner Emotions for Online Learning in Video Conference Applications

Nika Qisty Fatharani[1], Asyifa Imanda Septiana[1,2]*, Raditya Muhammad[1], Yulia Retnowati[1] and Yusep Rosmansyah[2]

[1]Software Engineering, Kampus Cibiru, Universitas Pendidikan Indonesia, Bandung, Indonesia
[2]School of Electrical Engineering and Informatics, Institut Teknologi Bandung, Indonesia of Electrical Engineering and Informatics, Bandung Institute of Technology, Bandung 40132, Indonesia

ABSTRACT

Research on facial emotion recognition for learners has been conducted widely. However, research on how to deal with emotions detected during learning with computer systems has not been widely conducted. Therefore, this study aimed to develop a personalized verbal affective intervention through motivational messages to help learners regulate their negative emotions (sadness, anger, fear, and disgust). The system is developed for higher education learners on the Google Meet video conferencing application for online learning activities. The system was tested on 32 learners of Software Engineering at Universitas Pendidikan Indonesia. The learners were asked to fill out the Instructional Materials Motivation Survey (IMMS) questionnaire after the learning process to measure their learning motivation. Based on the questionnaire results, it can be concluded that personalized affective intervention, considering the ARCS Model, positively impacts learners' motivation during synchronous online learning. This study suggests that a learning intervention based on the learner's emotion recognition can positively affect the learner's motivation and experience in using video conferencing apps during synchronous learning. This study can be a valuable reference for future research in implementing ARCS aspects that match learners' emotional and emergent algorithms of affective interventions.

Keywords: Affective computing, emotion recognition, online learning, web application

ARTICLE INFO

Article history:
Received: 30 April 2025
Published: 17 July 2025

DOI: https://doi.org/10.47836/pp.1.3.006

E-mail addresses:
nikaqistyfatharani@gmail.com (Nika Qisty Fatharani)
asyifa@upi.edu (Asyifa Imanda Septiana)
radityamuhammad@upi.edu (Raditya Muhammad)
yulia.retnowati@upi.edu (Yulia Retnowati)
yusep@stei.itb.ac.id (Yusep Rosmansyah)
* Corresponding author

INTRODUCTION

In synchronous online learning, the use of video-conferencing applications is prevalent in replicating traditional classroom learning (Henriksen et al., 2020; Mouheb et al., 2022). Learners often experience negative

e-ISSN: 3083-9475

emotions due to the self-directed nature of online learning, physical and psychological separation without direct contact with educators and peers, which may hinder their learning process and outcomes (Deublein et al., 2018; Kouahla et al., 2023; Lee et al., 2021; Marchand & Gutierrez, 2012). Meanwhile, the emotion recognition process is related to affective computing because it aims to recognize a person's affective state, which is then analyzed to create an appropriate response (Yadegaridehkordi et al., 2019). Many studies have been conducted on FER technology in learning activities. However, this system has not been able to provide adaptive and personalized responses or feedback based on the learner's detected emotional states (Septiana et al., 2024).

Affective interventions can play a role in improving a learner's self-awareness, self-regulation, empathy, and social skills, which are important for well-being and academic success (Hasson-Ohayon et al., 2006; Oliveira et al., 2021).

Based on the background described, this research will focus on implementing effective interventions in the browser extensions used by learners. Affective interventions are provided through verbal motivational messages designed based on the ARCS Model to address negative emotions detected in learners' facial expressions. Affective intervention is provided according to each learner's preference for synchronous online learning. Providing effective intervention according to each learner's preference is expected to positively impact the learner's experience using video-conferencing applications in synchronous online learning activities to motivate the learner and create a more positive learning environment to achieve maximum learning outcomes.

METHOD

Motivational messages have been developed to address four negative emotions in online learning activities: Sadness, anger, fear, and disgust. Learners' facial expressions were analyzed to classify their emotions. The system performs emotion recognition for the user every 5 seconds with the support of face-api. js. Learners will receive motivational messages based on the learners' personality questionnaire data and their current emotions. The motivational message pop-up will be displayed for 5 seconds. The system was tested on 32 learners in a 120-minute learning course. Then they asked to fill out the Instructional Materials Motivation Survey (IMMS) questionnaire

RESULT AND DISCUSSION

Each of the total average values of the ARCS aspects received the "High" criteria as shown in Figure 1. In addition, according to the learners, affective intervention was considered relevant to the emotions they felt (relevance). This indicates that motivational messages designed by considering the learner's emotional state, linking the emotional state to personal skills and learning objectives, matching interests, and using analogies can make the intervention highly relevant for the learner.

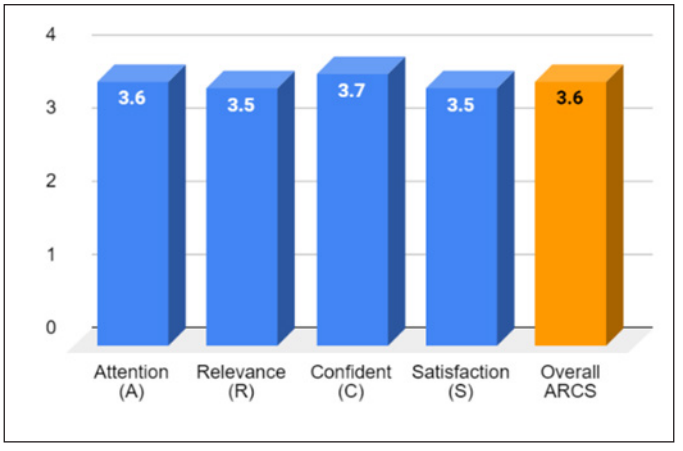

Figure 1. Result of system evaluation based on IMMS

CONCLUSION

The development of affective interventions aims to address the negative emotional states that arise during synchronous learning activities by providing motivational messages that are personalized according to learner preferences and personality. Based on the IMMS test results, the implementation of the ARCS Model as an effective intervention design strategy had a significant positive impact on learners' learning motivation and experience in using video conferencing applications for synchronous online learning activities. Other factors such as personality, communication preferences, or previous learning experiences may influence the outcome of the learner's motivation level and learning experience to affective intervention. The results of this study can be developed into further research related to examining which aspects of the ARCS Model are most suitable for dealing with each negative emotion.

ACKNOWLEDGEMENT

We express sincere gratitude to the Research and Community Service Institute of Universitas Pendidikan Indonesia for providing funding support through the 2024 Annual Work and Budget Plan Assignment Fund, in accordance with Rector's Decree Number: 392 / UN40/PT.01/2024. This support has been instrumental in the implementation and completion of this research.

REFERENCES

Deublein, A., Pfeifer, A., Merbach, K., Bruckner, K., Mengelkamp, C., & Lugrin, B. (2018). Scaffolding of motivation in learning using a social robot. *Computers & Education*, *125*, 182–190. https://doi.org/10.1016/j.compedu.2018.06.015

Hasson-Ohayon, I., Kravetz, S., Roe, D., Rozencwaig, S., & Weiser, M. (2006). Qualitative assessment of verbal and non-verbal psychosocial interventions for people with severe mental illness. *Journal of Mental Health*, *15*(3), 343–353. https://doi.org/10.1080/09638230600700847

Henriksen, D., Creely, E., & Henderson, M. (2020). Folk pedagogies for teacher educator transitions: approaches to synchronous online learning in the wake of COVID-19. *Journal of Technology and Teacher Education*, *28*(2), 201-209.

Kouahla, M. N., Boughida, A., Chebata, I., Mehenaoui, Z., & Lafifi, Y. (2023). Emorec: A new approach for detecting and improving the emotional state of learners in an e-learning environment. *Interactive Learning Environments*, *31*(10), 6223–6241. https://doi.org/10.1080/10494820.2022.2029494

Lee, J., So, H. J., Ha, S., Kim, E., & Park, K. (2021). Unpacking academic emotions in asynchronous video-based learning: focusing on Korean learners' affective experiences. *The Asia-Pacific Education Researcher*, *30*(3), 247–261. https://doi.org/10.1007/s40299-021-00565-x

Marchand, G. C., & Gutierrez, A. P. (2012). The role of emotion in the learning process: Comparisons between online and face-to-face learning settings. *The Internet and Higher Education*, *15*(3), 150–160. https://doi.org/10.1016/j.iheduc.2011.10.001

Mouheb, K., Yürekli, A., Dervisbegovic, N., Mohammed, R. A., & Yilmazel, B. (2022). EduFERA: A real-time student facial emotion recognition approach. *European Journal of Science and Technology*, (32), 690-695. https://doi.org/10.31590/ejosat.1039184

Oliveira, S., Roberto, M. S., Pereira, N. S., Marques-Pinto, A., & Veiga-Simão, A. M. (2021). Impacts of social and emotional learning interventions for teachers on teachers' outcomes: A systematic review with meta-analysis. *Frontiers in Psychology*, *12,* Article 677217. https://doi.org/10.3389/fpsyg.2021.677217

Septiana, A. I., Mutijarsa, K., Putro, B. L., & Rosmansyah, Y. (2024). Emotion-related pedagogical agent: A systematic literature review. *IEEE Access*, *12*, 36645–36656. https://doi.org/10.1109/ACCESS.2024.3374376

Yadegaridehkordi, E., Noor, N. F. B. M., Ayub, M. N. B., Affal, H. B., & Hussin, N. B. (2019). Affective computing in education: A systematic review and future research. *Computers & Education*, *142*, Article 103649. https://doi.org/10.1016/j.compedu.2019.103649

Pertanika Proceedings 1 (3): 31 - 37 (2025)

PERTANIKA JOURNALS

PERTANIKA PROCEEDINGS

Journal homepage: http://www.pertanika.upm.edu.my/

Performance Analysis of an OAuth 2.0-Based Authentication and Authorization System Using a Redis In-memory Database

Akbar Mahmudin, Hendriyana* and Mochamad Iqbal Ardimansyah

Department of Software Engineering, University Pendidikan Indonesia, 229 Dr. Setiabudi Street, Bandung 40514, West Java, Indonesia

ABSTRACT

The OAuth 2.0 framework is a protocol that allows third-party applications to gain authorized access to user resources. However, inefficient token management and storage can adversely affect the workload of OAuth 2.0 systems, especially when system traffic is high, such as performance degradation, slow response time and security vulnerabilities. Therefore, token management and storage are essential in the OAuth 2.0 ecosystem to ensure user security and convenience. This research aims to analyze the impact of Redis in-memory database implementation on token management on OAuth 2.0 system performance. In addition, the research focuses on the results of load testing conducted on the OAuth 2.0 system, referring to software quality based on performance efficiency in accordance with ISO 25010, including aspects of time response, throughput and resource utilization. Load testing simulates the authentication and authorization process using the OAuth 2.0 system to observe the effect after the implementation of Redis in token management at user load levels of 100, 300, and 500. The results show that Redis has an influence on the performance of the OAuth 2.0 system on response time, throughput, and memory usage. On the aspect of CPU usage, it does not show any influence, even after Redis is implemented. The advantages of Redis can be attributed to the memory-based storage that enables faster read-write operations, especially for single data with low latency.

Keywords: Authentication, authorization, IMDB, OAuth, Redis

ARTICLE INFO

Article history:
Received: 30 April 2025
Published: 17 July 2025

DOI: https://doi.org/10.47836/pp.1.3.007

E-mail addresses:
akbarmahmudin@upi.edu (Akbar Mahmudin)
hendriyana@upi.edu (Hendriyana)
iqbalardimansyah@upi.edu (Mochamad Iqbal Ardimansyah)
* Corresponding author

INTRODUCTION

OAuth 2.0 is one of the most popular authentication and authorization protocols as it allows third-party applications to gain legitimate access to user resources without the need to reveal user passwords (Kiani,

2020). The Authorization Code Grant offers enhanced security benefits due to the fact that the authorization code is transmitted exclusively over a secure channel between the client and the OAuth server (Fett et al., 2016). Inefficient token storage can result in performance degradation, longer response times, and even potential security vulnerabilities (Safaryan et al., 2020). Therefore, there is a need for a database system that can efficiently store and manage tokens.

One type of database with fast read performance is an in-memory database, where all information is stored in main memory (Kausar et al., 2022; Safaryan et al., 2020). When it comes to storing data that is stored and retrieved from volatile memory, Redis has better performance than Memcached in terms of data persistence and handling heavy traffic loads (Alami et al., 2018). In addition, Redis has the best read performance of MongoDB and Cassandra (Kausar et al., 2022; Kabakus & Kara, 2017). This is due to Redis's ability to access data with very low latency. With faster and more efficient request response, Redis has the potential to improve user experience in the OAuth 2.0 ecosystem in system performance.

PROBLEM STATEMENT

The research implements the Authorization Code Grant flow using the Redis in-memory database as a token database, with the aim of analyzing the performance of the OAuth 2.0-based authentication and authorization system. This will entail an in-depth examination of the system's response time, throughput, and utilization (Li et al., 2017; Wang & Wu, 2019; Zulfa et al., 2020). The objective of this study is to conduct a comprehensive examination of the operational efficacy of the Redis system (Tkachenko & Lukianiuk, 2021). The research reference for subsequent investigations that may undertake a comparative analysis of Redis with other IMDBs.

RESEARCH QUESTIONS

On the server side or backend, using a microservices architecture shown in Figure 1.

Testing will be conducted on the backend or server side of the OAuth 2.0 system (Auth Server) using load testing to test each system performance metric, namely response time, throughput, CPU usage and memory usage. The description of each metric used in this study is as follows:

1. Average response time (M1) required by the OAuth 2.0 system to respond to a user or task (Equation 1).

$$X = \sum_{i=1\ ke\ n} \frac{A_i}{n} \qquad [1]$$

Ai = time required by the OAuth 2.0 system, *n* = number of responses

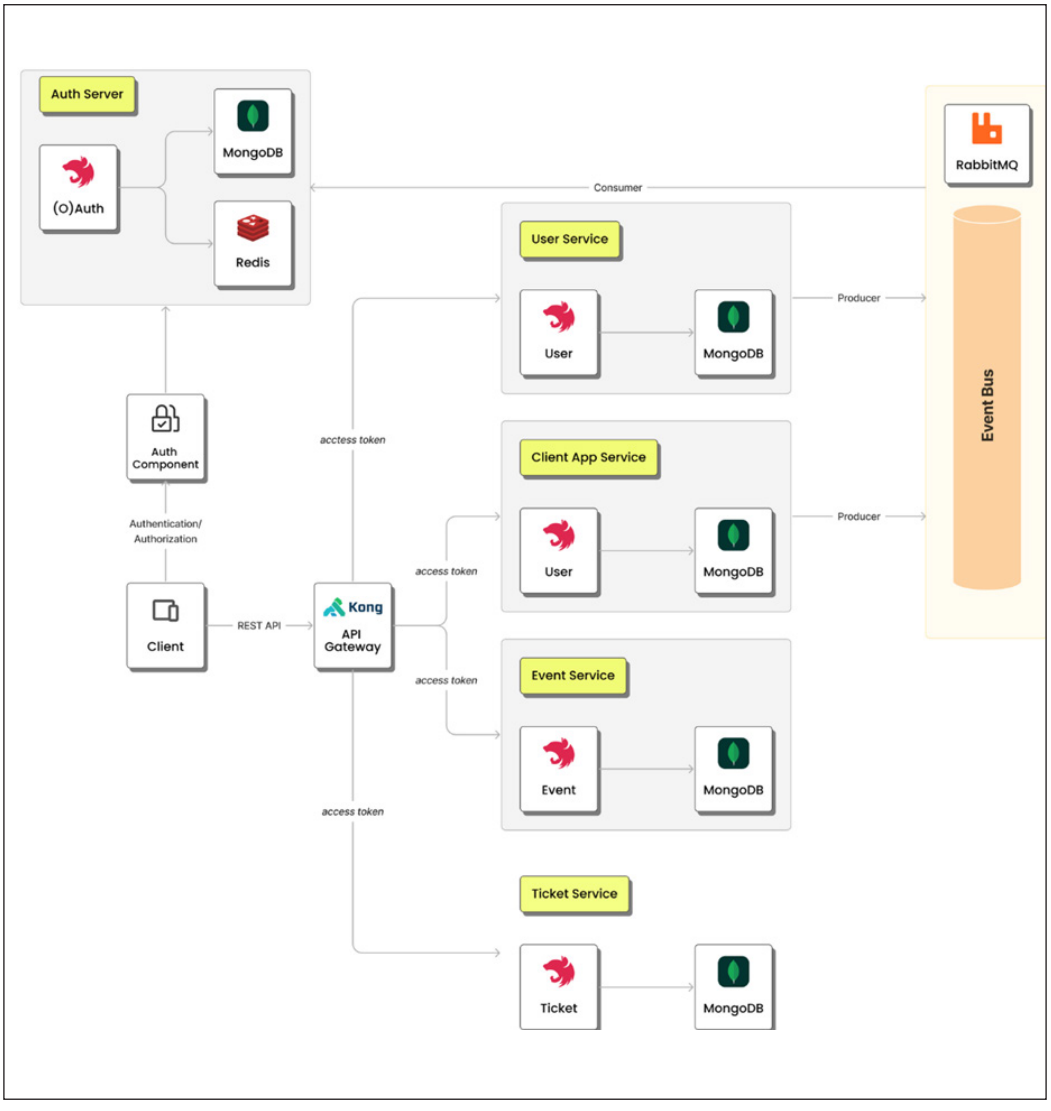

Figure 1. System architecture

2. Average throughput (M2) that the OAuth 2.0 system can process in a unit of time (seconds) (Equation 2).

$$X = \sum_{i=1\ ke\ n} \frac{A_i / B_i}{n} \qquad [2]$$

Ai = number of commands successfully processed, *Bi* = time to execute a command

3. Average CPU usage (M3) when executing commands within a certain period (Equation 3).

$$X = \sum_{i=1\ ke\ n} \frac{A_i/B_i}{n} \quad [3]$$

Ai = CPU usage size to execute a command, *Bi* = operation time to execute a command

4. Average memory usage (M4) when executing a command in a certain period (Equation 4).

$$X = \sum_{i=1\ ke\ n} \frac{A_i/B_i}{n} \quad [4]$$

Ai = memory usage size to execute a command, *Bi* = memory usage time to execute a command

The tests were conducted by incrementally increasing the load based on the number of virtual users, i.e., 100, 300, and 500 users simultaneously within 300 seconds (Suryawana & Muliantaraa, 2024). Based on previous research, this number can identify and address potential bottlenecks and performance issues without overloading the system in the early stages of testing (Tkachenko & Lukianiuk, 2021). Figure 2 is a scenario that simulates the user authentication and authorization process on a third-party application.

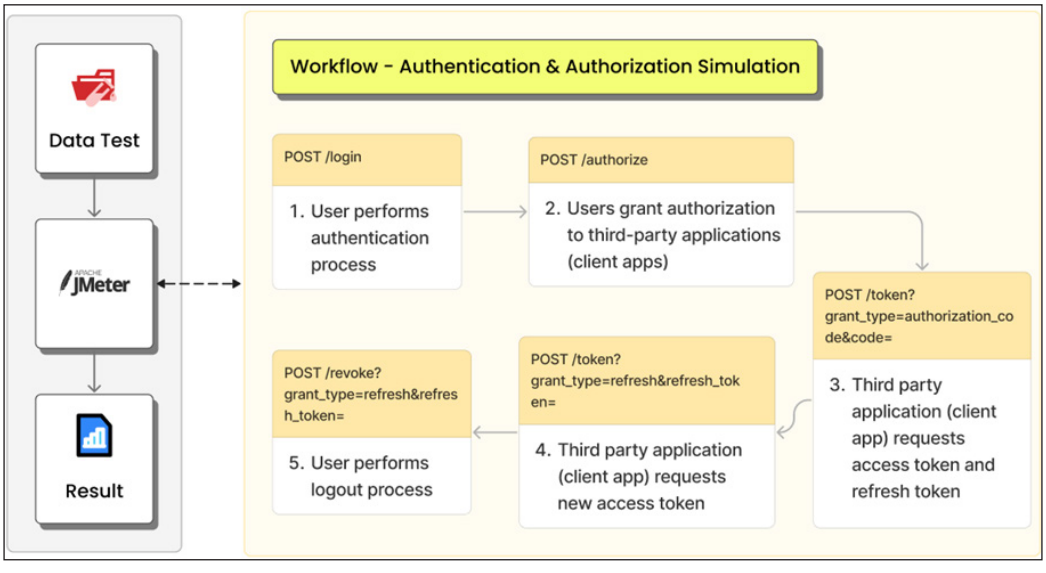

Figure 2. Testing scenario

The findings of the research conducted on load testing the OAuth 2.0 system under two different conditions to assess the impact of implementing Redis in the OAuth 2.0 system on response time, throughput, CPU usage and memory usage. The condition before implementing Redis is named pre-Redis, and after implementing Redis is named post-Redis.

1. Time Response Aspect (M1)
   The average response time of the OAuth 2.0 system shows a significant performance improvement, with a load of 100 showing an increase of 9.18%, a load of 300 showing an increase of 6.41%, and a load of 500 showing an increase of 4.06%. Figure 3 below provides a visualization of the performance improvement of both OAuth 2.0 system conditions.
2. Throughput Aspect (M2)
   The OAuth 2.0 system shows significant performance improvement, with load 100 showing an increase of 7.75%, load 300 showing an increase of 5.10%, and load 500 showing an increase of 3.14%. Figure 4 visualizes throughput aspect observations, demonstrating that the post-Redis system condition is capable of handling a greater number of requests per second.
3. CPU Usage Aspect (M3)
   The performance improvement is not as significant, with load 100 only showing a 1.54% improvement, load 300 showing a lower improvement of 0.16%, and load 500 showing a 1.67% improvement based on the average CPU usage. Figure 5 provides

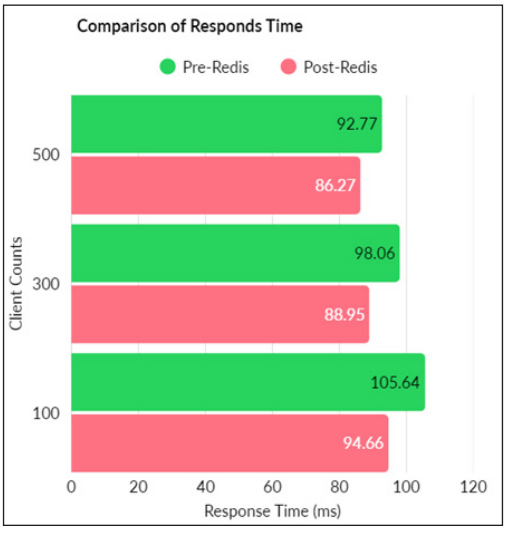

Figure 3. Bar chart of scenario M1 for each load

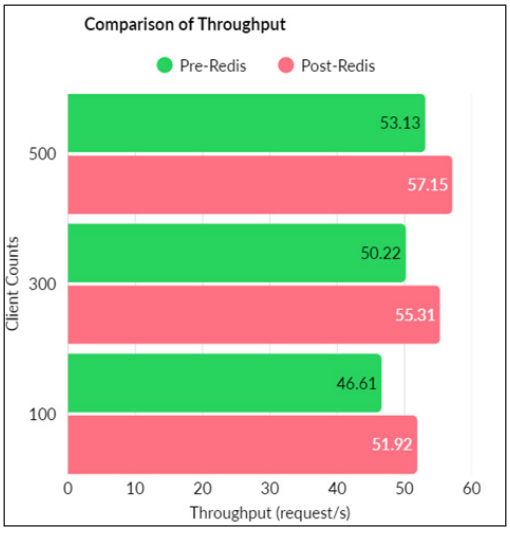

Figure 4. Bar chart of scenario M2 for each load

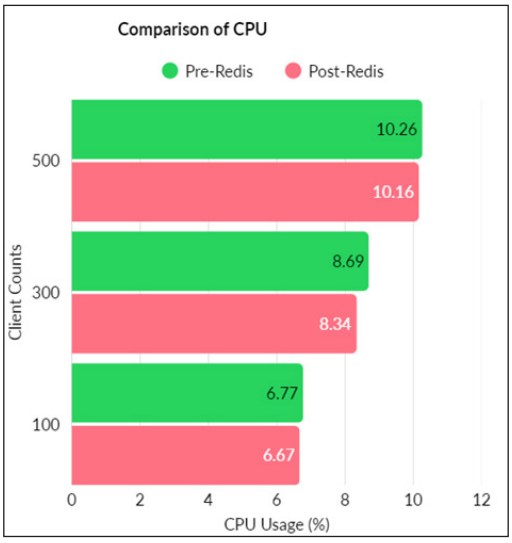

Figure 5. Bar chart of scenario M3 for each load

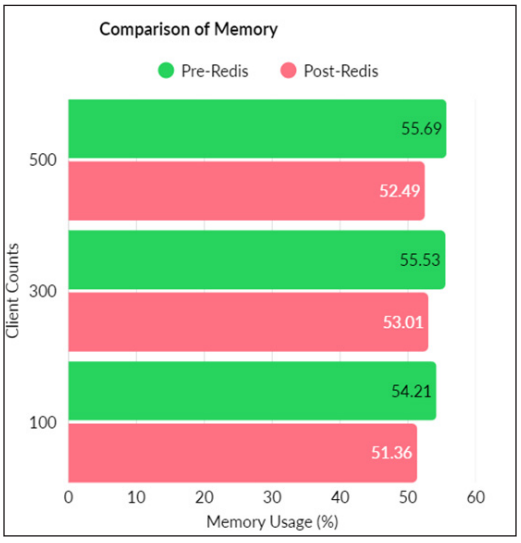

Figure 6. Bar chart of scenario m4 for each load

a visualization of the CPU usage of both system conditions at each load. CPU usage aspects reveal a consistent and gradual increase in CPU usage over a period, with a slight decrease over time, in both system conditions.

4. Memory Usage Aspect (M4)
   Figure 6 is a visual representation of the comparison between the two system conditions. This system condition exhibits superiority across various types of loads, including the highest loads. This aspect does not require further discussion, given that Redis is an in-memory database that stores all data in RAM.

CONCLUSION

A major challenge faced in the OAuth 2.0 ecosystem is the efficient storage and management of tokens. This research is motivated by the flexibility of the OAuth 2.0 standard and the performance reliability of the in-memory database Redis, which has the potential to access token data with very low latency and with faster and more efficient request response. The results show that the implementation of Redis in token management in OAuth 2.0-based authentication and authorization systems has an effect on response time, throughput, and memory usage. However, there is no significant effect on the CPU usage aspect after the Redis implementation. When viewed from the largest load, the percentage of performance improvement in the aspect of response time increased by 4.06%, throughput increased by 3.14%, CPU usage increased by 1.67%, and memory usage increased by 2.87%. The superiority of Redis in almost all aspects can be attributed to the memory-based storage that enables faster read/write operations, especially for single data with low latency.

ACKNOWLEDGEMENT

This research was supported by the Universitas Pendidikan Indonesia under research grant No. 385/UN40.LP/PT.01.03/2024. We also acknowledge the Software Engineering Study Program for providing access to laboratory facilities during this study.

REFERENCES

Alami, A. E., Bahaj, M., & Khourdifi, Y. (2018). Supply of a key value database redis in-memory by data from a relational database. In *2018 19th IEEE Mediterranean Electrotechnical Conference (MELECON)* (pp. 46-51). IEEE. https://doi.org/10.1109/MELCON.2018.8379066

Fett, D., Küsters, R., & Schmitz, G. (2016). A comprehensive formal security analysis of OAuth 2.0. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1204-1215). ACMDL https://doi.org/10.1145/2976749.2978385

Kabakus, A. T., & Kara, R. (2017). A performance evaluation of in-memory databases. *Journal of King Saud University - Computer and Information Sciences*, *29*(4), 520–525. https://doi.org/10.1016/j.jksuci.2016.06.007

Kausar, M. A., Nasar, M., & Soosaimanickam, A. (2022). A study of performance and comparison of nosql databases: Mongodb, cassandra, and redis using ycsb. *Indian Journal of Science and Technology*, *15*(31), 1532–1540. https://doi.org/10.17485/IJST/v15i31.1352

Kiani, K. (2020). *How to secure your oauth implementation*. Citeseer. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=dbd29ff47bb6b600e24250d9e4a34d985e044537

Li, S., Jiang, H., & Shi, M. (2017). Redis-based web server cluster session maintaining technology. In *2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)* (pp. 3065-3069). IEEE. https://doi.org/10.1109/FSKD.2017.8393274

Safaryan, O., Pinevich, E., Roshchina, E., Cherckesova, L., & Kolennikova, N. (2020). Information system development for restricting access to software tool built on microservice architecture. *E3S Web of Conferences*, *224*, Article 01041. https://doi.org/10.1051/e3sconf/202022401041

Suryawana, A. I., & Muliantaraa, A. (2024). Database performance optimization using lazy loading with Redis on online marketplace website. *Jurnal Elektronik Ilmu Komputer Udayana P-ISSN*, *2301*, Article 5373.

Tkachenko, V., & Lukianiuk, S. (2021). Analysis of the use of the Redis in the distributed order processing system in the restaurant network. *Technology Audit and Production Reserves*, *5*(2), 39-43. https://doi.org/10.15587/2706-5448.2021.238460

Wang, J., & Wu, J. (2019). Research on performance automation testing technology based on JMeter. In *2019 International Conference on Robots & Intelligent System (ICRIS)* (pp. 55-58). IEEE. https://doi.org/10.1109/ICRIS.2019.00023

Zulfa, M. I., Fadli, A., & Wardhana, A. W. (2020). Application caching strategy based on in-memory using Redis server to accelerate relational data access. *Jurnal Teknologi dan Sistem Komputer*, *8*(2), 157–163. https://doi.org/10.14710/jtsiskom.8.2.2020.157-163

Pertanika Proceedings 1 (3): 39 - 44 (2025)

PERTANIKA JOURNALS

PERTANIKA PROCEEDINGS

Journal homepage: http://www.pertanika.upm.edu.my/

Website Security Using Next.js: An Analytical Approach with OWASP Top 10

Raditya Muhammad*, Reihan Manzis Syahputra and Mochamad Iqbal Ardimansyah

Department of Software Engineering, Cibiru Regional Campus, Universitas Pendidikan Indonesia, Bandung 40393, Indonesia

ABSTRACT

This research investigates the effectiveness of Next.js in enhancing web application security, focusing on the IdeaBox Multi-Tenant platform, an idea and innovation collaboration tool. The study adopts an analytical approach referencing OWASP Top 10 and employs Zed Attack Proxy (ZAP) tools, such as Ajax spider and active scan for vulnerability testing. The objective is to measure the impact of Next.js features on mitigating security risks. Initial testing identified 12 security vulnerabilities, including Broken Access Control, Cryptographic Failures, and Security Misconfigurations. After implementing Next.js features like Server-Side Rendering, Middleware, Formik, Yup Validation, Nookies, and bcrypt, the vulnerabilities were reduced to seven categories, with significant risk reduction. The results highlight how Next.js features enhance input validation, data protection, and overall security. This study demonstrates that integrating Next.js effectively minimizes vulnerabilities and improves website security, offering practical guidance for developers. The research underscores the importance of advanced frameworks in mitigating cyber threats and safeguarding sensitive user data.

Keywords: Cyber attacks, OWASP top 10, website security

INTRODUCTION

Website applications, providing essential services. However, as their importance grows, so does the threat to the security of data they handle (Hassan et al., 2023). With web applications often storing sensitive information, robust security testing becomes crucial to prevent cyber attacks (Fata, 2023; Ghelani, 2023; Risky & Yuhandri, 2021).

ARTICLE INFO

Article history:
Received: 30 April 2025
Published: 17 July 2025

DOI: https://doi.org/10.47836/pp.1.3.008

E-mail addresses:
radityamuhammad@upi.edu (Raditya Muhammad)
reihanmanzis@upi.edu (Reihan Manzis Syahputra)
iqbalardimansyah@upi.edu (Mochamad Iqbal Ardimansyah)
* Corresponding author

e-ISSN: 3083-9475

The rise of cyber attacks aimed at compromising data integrity and confidentiality poses significant operational risks (Febryanti et al., 2023).

The IdeaBox platform is vulnerable to common web application threats. To mitigate these risks, the adoption of advanced web development frameworks, such as Next.js, is essential (Lazuardy & Anggraini, 2022). Next.js, a React-based framework, enables the creation of responsive, fast, and secure web applications through features like server-side rendering (Jartarghar et al., 2022), dynamic routing, and Middleware (Dinku, 2022).

Problem Statement

Cyber attacks targeting data integrity and confidentiality pose operational risks (Willberg, 2019), particularly for IdeaBox, which stores sensitive data. While frameworks like Next.js offer advanced security capabilities, there is limited research on their effectiveness in addressing common vulnerabilities identified in the OWASP Top 10 framework (OWASP, 2021; Abdan, 2022). This lack of focused analysis leaves a gap in understanding how Next.js impacts web application security.

Research Question

This study seeks to address the following questions: How do Next.js features impact the application's security level? Finally, to what extent can the integration of Next.js features reduce risks associated with prevalent web application threats? These questions aim to provide a comprehensive understanding of the role of Next.js in enhancing web application security.

METHODOLOGY

The research was conducted in four stages. First, a website domain was selected for testing. Second, the IdeaBox Multi-tenant application, built with React.js and Laravel, was tested using Zed Attack Proxy (ZAP) (Kalaani, 2023) with AJAX Spider and Active Scan methods to identify security vulnerabilities. Third, Next.js features, such as Server-Side Rendering, Middleware, Formik, Yup, Nookies, and bcrypt, were implemented to enhance security. Finally, the application was retested using ZAP's Automated Scan to assess the impact of these Next.js features on reducing security vulnerabilities.

RESULTS AND DISCUSSION

The IdeaBox Multi-Tenant application implemented Next.js features and relevant libraries, including server-side rendering, middleware, Formik, Yup Validation, Nookies, and bcrypt. Security testing was conducted using OWASP guidelines and Zed Attack Proxy (ZAP) tools, employing Ajax Spider and Active Scan methods to identify vulnerabilities and threats as shown in Table 1.

Table 1
Vulnerability after implementing Next.js features

No	Vulnerability Name	Risk level	Qty
1	Content Security Policy (CSP) Header Not Set	Medium	1
2	Missing Anti-Clickjacking Header	Medium	1
3	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	1
4	X-Content-Type-Options Header Missing	Low	33
5	Information Disclosure-Suspicious Comments	Informational	89
6	Modern Web Applications	Informational	1
7	User Agent Fuzzer	Informational	132

The vulnerability analysis is based on the OWASP Top 10 method (Table 2). In the Broken Access Control category, vulnerabilities like server information disclosure via “X-Powered-By” HTTP headers and suspicious source code comments were noted, potentially aiding attackers. The Cryptographic Failures category further highlighted risks of sensitive data exposure. Security Misconfiguration vulnerabilities, including missing headers (CSP, Anti-clickjacking, X-Content-Type-Options), increased risks of XSS attacks, Clickjacking, and content type manipulation, underscore the need for mitigation strategies aligned with NIST’s CVSS framework (Mell et al., 2006).

Table 2
OWASP top 10 vulnerability categorization on testing after next.js implementation

OWASP	Categories	Name	Qty
A01	Broken Access Control	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1 detected) Information Disclosure-Suspicious Comments (89 detected)	2
A02	Cryptographic Failures	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1 detected) Information Disclosure-Suspicious Comments (89 detected)	2
A05	Security Misconfiguration	Content Security Policy (CSP) Header Not Set (1 detected), Missing Anti-clickjacking Header (1 detected), X-Content-Type-Options Header Missing (33 detected)	3

The evaluation in Table 3 reveals that the IdeaBox Multi-Tenant application still faces moderate-risk vulnerabilities, including Broken Access Control (CVSS 5.1), Cryptographic Failures (5.2), and Security Misconfiguration (6.4). While Next.js features have reduced some risks, exploitable gaps remain, necessitating additional security measures, continuous monitoring, and further integration with complementary security technologies.

Table 3
Vulnerability risk level after implementing Next.js features

No	Vulnerability Category	CVSS Score	Status
1	Broken Access Control	5.1	Medium
2	Cryptographic Failures	5.2	Medium
3	Injection	N/A	N/A
4	Insecure Design	N/A	N/A
5	Security Misconfiguration	6.4	Medium
6	Vulnerable and Outdated Components	N/A	N/A
7	Identification and Authentication Failures	N/A	N/A
8	Software and Data Integrity Failures	N/A	N/A
9	Security Logging and Monitoring Failures	N/A	N/A
10	Server-Side Request Forgery (SSRF)	N/A	N/A

Table 4 shows that after implementing Next.js security features, vulnerabilities in the IdeaBox Multi-tenant website vary in likelihood, with Broken Access Control scoring low (2,875), and Cryptographic Failures and Security Misconfiguration scoring medium (4,375 and 5,750).

Table 4
Likelihood level after implementing Next.js features

No	Vulnerability Category	Likelihood Score	Likelihood Level
1	Broken Access Control	2,875	Low
2	Cryptographic Failures	4,375	Medium
3	Injection	N/A	N/A
4	Insecure Design	N/A	N/A
5	Security Misconfiguration	5,750	Medium
6	Vulnerable and Outdated Components	N/A	N/A
7	Identification and Authentication Failures	N/A	N/A
8	Software and Data Integrity Failures	N/A	N/A
9	Security Logging and Monitoring Failures	N/A	N/A
10	Server-Side Request Forgery (SSRF)	N/A	N/A

The implementation of Next.js features reduced the IdeaBox Multi-Tenant application's risk level from high (7.9) to medium (5.57), with a significant drop in vulnerabilities. Low-risk findings decreased from 246 to 34, medium-risk findings from 248 to 2, and no high-risk vulnerabilities remained. OWASP Top 10 issues like Broken Access Control and Security Misconfiguration were significantly mitigated, and Identification and Authentication Failures were eliminated. These results demonstrate the effective use of Next.js features in enhancing application security.

CONCLUSION

The implementation of Next.js significantly improved the security of the IdeaBox Multi-Tenant application, reducing vulnerabilities from 12 to 7 categories with lower risks. Features like Server-Side Rendering, Middleware, Formik, Yup Validation, Nookies, and bcrypt effectively addressed data handling, access control, input validation, and encryption. The OWASP Top 10 framework and CVSS were instrumental in assessing risks. While security was enhanced, some gaps remain, requiring ongoing monitoring and further mitigation.

ACKNOWLEDGEMENT

We sincerely appreciate the support and provision of essential resources from Universitas Pendidikan Indonesia, which significantly contributed to the development of this project.

REFERENCES

Abdan, M. K. (2022). *Web-Based Information System Security Testing Based on the OWASP WSTG V4.2 Framework (Case study: Sekawan System V1)*. Universitas Islam Indonesia.

Dinku, Z. (2022). *React.js vs. Next.js* [Unpublish bachelor's thesis]. Metropolia University of Applied Sciences.

Fata, D. (2023). *Evaluation of Security Vulnerability Risk Using OWASP Methodology on Academic Information System Web Applications UIN AR-RANIRY*. Universitas Islam Negeri Ar-Raniry.

Febryanti, P. C., Subartini, B., & Riaman, R. (2023). Calculation of cyber risk level in digital financial services based on aggregate loss costs. *FIBONACCI: Jurnal Pendidikan Matematika Dan Matematika*, *9*(1), 95–104.

Ghelani, D. (2022). Cyber security, cyber threats, implication and future perspectives: A review. *American Journal of Science, Engineering and Technology*, *3*(6), 12–19.

Hassan, A. A., Rony, M. A., Yuliazmi, & Putra, B. C. (2023). E-commerce implementation using content management system (CMS) at Linda Collection Store. *2nd Seminar Nasional Mahasiswa Fakultas Teknologi (Senafti), 2*(1), 659–667.

Jartarghar, H. A., Salanke, & Dalali, S. (2022). React Apps with server-side rendering: Next.js. *Journal of Telecommunication, Electronic and Computer Engineering*, *14*(4), 25–29. https://doi.org/10.54554/jtec.2022.14.04.005

Kalaani, C. (2023). *OWASP ZAP vs Snort for SQLi Vulnerability Scanning*. Georgia Southern University.

Lazuardy, M. F. S., & Anggraini, D. (2022). Modern front end web architectures with React.Js and Next.Js. *International Research Journal of Advanced Engineering and Science*, *7*(1), 132–141.

Mell, P., Scarfone, K., and Romanosky, S. (2006). Common vulnerability scoring system. *IEEE Security & Privacy, 4*(6), 85-89. https://doi.org/10.1109/MSP.2006.145

OWASP. (2021). *OWASP Top 10:2021*. Open Web Application Security Project. https://owasp.org/Top10/

Risky, M. A. Z., & Yuhandri, Y. (2021). Optimization in website security penetration testing using SQL injection and XSS techniques. *Jurnal Sistim Informasi dan Teknologi, 3*(4), 215–220. https://doi.org/10.37034/jsisfotek.v3i4.68

Willberg, M. (2019). *Web application security testing with owasp top 10 framework* [Unpublished bachelor's thesis]. Turku University of Applied Science.

Pertanika Proceedings 1 (3): 45 - 49 (2025)

PERTANIKA JOURNALS

PERTANIKA PROCEEDINGS

Journal homepage: http://www.pertanika.upm.edu.my/

Minimizing Face Spoofing Attacks with Liveness Detection in Cross-Platform Mobile Attendance Systems

Bagus Subagja, Dian Anggraini* and Asyifa Imanda Septiana

Software Engineering, Kampus Cibiru, Universitas Pendidikan Indonesia, 40625 Bandung, Jawa Barat, Indonesia

ABSTRACT

Attendance systems have now implemented many of the most recent technologies, such as the use of facial recognition to verify and validate student attendance in lecture classes. However, face recognition technology in the attendance systems is still prone to fraud with attacks using artificial faces through various media, such as printed photos or pre-recorded videos. Therefore, a liveness detection system is needed that can minimize the fraud. The liveness detection system using the randomized challenge-response method, with several randomly given challenges within a time limit, can indicate whether the detected face is genuinely alive. This liveness detection system is implemented in a cross-platform mobile-based digital attendance application called "My Attendance" developed using the Flutter framework. Student attendance records are stored and can be viewed by lecturers as proof of attendance in lecture classes. The results of the study show that this liveness detection system can minimize the occurrence of fraudulent artificial face attacks, achieving 100% performance accuracy when tested on 30 respondents from students of the Software Engineering study program at the Indonesian Education University. This system could be an effective and efficient solution for applying face recognition systems to the attendance process.

Keywords: Attendance system, face spoofing attack, liveness detection, mobile cross-platform

ARTICLE INFO

Article history:
Received: 30 April 2025
Published: 17 July 2025

DOI: https://doi.org/10.47836/pp.1.3.009

E-mail addresses:
bagussubagja@upi.edu (Bagus Subagja)
dian.anggraini@upi.edu (Dian Anggraini)
asyifa@upi.edu (Asyifa Imanda Septiana)
* Corresponding author

INTRODUCTION

Technology nowadays has developed and influenced various fields in human life, which has become a necessity in daily activities. One of the fields that has implemented sophisticated technology now is the attendance system found in the educational environment that uses face recognition (Sunaryono et al., 2021).

e-ISSN: 3083-9475

Technology has advanced rapidly and has had a significant impact on many aspects of human life, becoming an essential part of daily activities. One notable field that has adopted sophisticated technology is the educational environment, where attendance systems now use facial recognition technology.

Problem Statement

However, face recognition systems are generally vulnerable to spoofing fraud (Hadiprakoso & Buana, 2021) because they frequently cannot distinguish between real and fake faces, creating a significant security risk (Chakraborty & Das, 2014). Spoofing is penetrating the recognition system's biometric authentication using fake face videos and printed photos (Karmakar et al., 2021; Khairnar et al., 2023).

Research Question

To mitigate spoofing attacks in face recognition systems, implementing liveness detection is crucial for distinguishing between real and fake faces (Li et al., 2018). Given that spoofing poses a significant threat to attendance systems using face recognition technology, research is needed to minimize attendance fraud (Singh & Arora, 2017; Ramachandra & Busch, 2017). This study focuses on two aspects: developing and analyzing a liveness detection system using randomized challenge-response methods for mobile cross-platform attendance systems, and examining the failure rate of attendance attempts using this system (Biørn-Hansen et al., 2018; Zohud & Zein, 2021). These objectives aim to enhance the security and reliability of facial recognition-based attendance while evaluating the effectiveness of the proposed solution (Kaur & Kaur, 2022).

SYSTEM DEVELOPMENT FOR LIVENESS DETECTION

Randomized Challenge Response Liveness Detection Methods

The research will assess the system's effectiveness using key performance metrics such as accuracy, precision, recall, and F-score, while also analyzing failure rates in attendance experiments to provide a comprehensive evaluation of real-world performance. Researchers will conduct testing based on these four scenarios, detailed in Table 1, to represent the capabilities of the liveness detection system under study, ensuring a thorough examination of its functionality and reliability in various conditions. The liveness detection process begins with a 45-second scan featuring six random challenges, each lasting approximately 7.5 seconds. If face detection fails, the process restarts to prevent spoofing. The system captures a final facial image after successful challenge completion. The testing scenarios are shown in Table 1.

Table 1
The test scenario is given to the participant

Scenario	Description	Notes
Scenario I	Students must attend using their actual faces, ensuring successful verification and attendance through real face detection.	All students are given 20 minutes to attend scenario I.
Scenario II	Students attempting attendance with artificial video faces should fail verification, as the liveness detection system will identify them as fake faces.	Testing with the face resulting from this artificial video recording is given a chance 3 times.
Scenario III	Students using their real faces should fail the attendance verification due to a system error or malfunction.	All students are given 20 minutes to attend scenario III.
Scenario IV	Students using artificial video faces with matched movements should fail verification, as the system should identify simulated faces despite mimicked liveness gestures.	Testing with the face resulting From this artificial video recording, it is given a chance 3 times.

RESULT AND DISCUSSION

Liveness Detection System Testing Results

Based on the results of the research survey in the previous point, the confusion matrix parameter values were obtained to evaluate the performance of the tested liveness detection as shown in Figure 1.

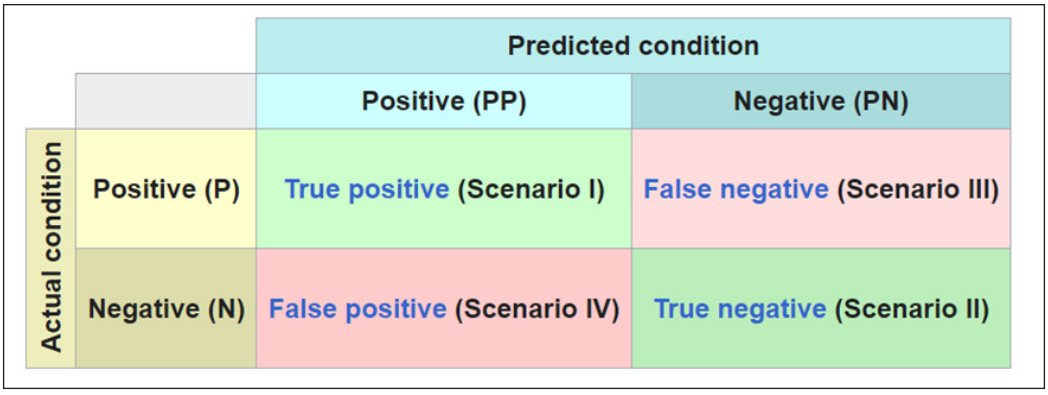

Figure 1. Testing scenarios and their relationship with confusion matrix values and the values obtained from discussion points of research survey results

The liveness detection system using a randomized challenge-response method achieved flawless results in testing, with 100% accuracy, precision, recall, and F-score. It effectively distinguished live faces from spoofing attempts without errors, proving its robustness and reliability. This highlights its potential as a highly secure solution for face recognition-based

systems, setting a new standard in liveness detection. During testing of a mobile attendance system's liveness detection, all 30 participants completed Scenarios I and III (real faces) within 20 minutes. Scenario I had a 33% initial failure rate (15/45 attempts), and Scenario III had a 23% rate (9/39 attempts). While all participants eventually succeeded, the results highlight the need to improve first-attempt success rates and system efficiency.

CONCLUSION

The liveness detection system achieved 100% accuracy in minimizing face spoofing attacks. However, analysis of Scenarios I and III revealed significant initial failure rates (33% and 23%, respectively) before all participants succeeded. While the system ultimately proved effective, these initial challenges across different conditions suggest room for improvement in consistency and user experience. The research demonstrates the system's overall success in preventing spoofing, but also highlights the need for refinements to reduce initial failures and enhance performance across various usage scenarios.

ACKNOWLEDGEMENT

The author is profoundly grateful to Universitas Pendidikan Indonesia (UPI) for the generous support and invaluable opportunity to undertake and complete this research. The resources and assistance provided by UPI have been pivotal to the successful completion of this project

REFERENCES

Biørn-Hansen, A., Grønli, T. M., & Ghinea, G. (2018). A survey and taxonomy of core concepts and research challenges in cross-platform mobile development. *ACM Computing Surveys (CSUR)*, *51*(5), 1-34. https://doi.org/10.1145/3241739

Chakraborty, S., & Das, D. (2014). An overview of face liveness detection. *International Journal on Information Theory*, *3*(2), 11–25. https://doi.org/10.5121/ijit.2014.3202

Hadiprakoso, R. B., & Buana, I. K. S. (2021). Deteksi serangan spoofing wajah menggunakan convolutional neural network. *Jurnal Teknik Informatika dan Sistem Informasi*, *7*(3), 618-626. https://doi.org/10.28932/jutisi.v7i3.4001

Karmakar, D., Mukherjee, P., & Datta, M. (2021). Spoofed facial presentation attack detection by multivariate gradient descriptor in micro-expression region. *Pattern Recognition and Image Analysis*, *31*(2), 285–294. https://doi.org/10.1134/S1054661821020097

Kaur, A., & Kaur, K. (2022). Systematic literature review of mobile application development and testing effort estimation. *Journal of King Saud University-Computer and Information Sciences*, *34*(2), 1-15. https://doi.org/10.1016/j.jksuci.2018.11.002

Khairnar, S., Gite, S., Kotecha, K., & Thepade, S. D. (2023). Khairnar, S., Gite, S., Kotecha, K., & Thepade, S. D. (2023). Face liveness detection using artificial intelligence techniques: A systematic literature review

and future directions. *Big Data and Cognitive Computing*, *7*(1), Article 37. https://doi.org/10.3390/bdcc7010037

Ramachandra, R., & Busch, C. (2017). Presentation attack detection methods for face recognition systems: A comprehensive survey. *ACM Computing Surveys*, 50(1), Article 8. https://doi.org/10.1145/3038924

Singh, M., & Arora, A. S. (2017). A robust anti-spoofing technique for face liveness detection with morphological operations. *Optik, 139*, 347–354. https://doi.org/10.1016/j.ijleo.2017.04.004

Sunaryono, D., Siswantoro, J., & Anggoro, R. (2021). An android based course attendance system using face recognition. *Journal of King Saud University - Computer and Information Sciences, 33*(3), 304–312. https://doi.org/10.1016/j.jksuci.2019.01.006

Zohud, T., & Zein, S. (2021). Cross-platform mobile app development in industry: A Multiple case-study. *International Journal of Computing*, *20*(1), 46–54. https://doi.org/10.47839/ijc.20.1.2091

Pertanika Proceedings 1 (3): 51 - 56 (2025)

PERTANIKA JOURNALS

PERTANIKA PROCEEDINGS

Journal homepage: http://www.pertanika.upm.edu.my/

Prediction Level of Software Maintainability Using Ensemble Method and Feature Selection

Indira Syawanodya*, Mochamad Iqbal Ardimansyah and Mochamad Nurul Huda

Software Engineering, UPI Regional Campus Cibiru, Universitas Pendidikan Indonesia, Bandung 40625, Indonesia

ABSTRACT

Software maintainability is a key external attribute of software quality that assesses how effectively and efficiently software can be modified by those who maintain it. The maintainability level is predicted using a machine learning model based on several software quality attributes, which can then be used to support decision-making during the software maintenance process. The previous research revealed that the generated predictive models for software maintainability levels still do not meet the established accuracy standards. This study discusses machine learning models built using several individual models, such as Lasso Regression, KNN, Regression Tree, M5Rules, SVM, and ANN, along with ensemble methods like Bagging and AdaBoost. Additionally, feature selection techniques are considered to identify the best features to improve the performance of the software maintainability prediction model. This study aims to investigate the performance of machine learning models in various datasets. The performance is evaluated using three metrics: MMRE, MAE, and Pred. The results show that the ANN algorithm is the best in almost all individual models with a score of MMRE 0,88. Ensemble methods have been proven to enhance the performance of models, given that the ensemble methods and individual algorithms used are appropriate. Feature selection techniques can improve some machine learning models by appropriately removing features, and the algorithms used match the data distribution with MMRE 0,84.

Keywords: Ensemble method, feature selection, individual model, software maintainability

ARTICLE INFO

Article history:
Received: 30 April 2025
Published: 17 July 2025

DOI: https://doi.org/10.47836/pp.1.3.010

E-mail addresses:
indira@upi.edu (Indira Syawanodya)
iqbalardimansyah@upi.edu (Mochamad Iqbal Ardimansyah)
mochamadnurulhuda16@gmail.com (Mochamad Nurul Huda)
* Corresponding author

INTRODUCTION

The capacity of a software product to satisfy explicit or implicit needs under predetermined circumstances is known as software quality. Although it cannot be assessed directly, software maintainability can be predicted using a model built on several internal software quality factors. (Land, 2002).

e-ISSN: 3083-9475

One measure of maintainability is maintenance effort, often gauged by the extent of changes needed (Alsolai & Roper, 2020). Accurate predictions of maintainability can aid decision-making, improve maintenance efficiency, compare project productivity and costs, and help with resource allocation (Elish & Elish, 2009). Various studies have proposed models using techniques like general regression neural networks (GRNN) (Thwin & Quah, 2005), Bayesian network (Koten & Gray, 2006), k-nearest neighbors (KNN) (Alsolai et al, 2018), and artificial neural networks (ANN) to predict software maintainability. However, many of these models still fail to meet accuracy standards (Alsolai & Roper, 2020). A reliable method to enhance model accuracy is by employing ensemble models, which integrate multiple individual models. (Alsolai et al, 2018). Feature selection techniques can also enhance model performance (Kumar et al., 2019).

This study uses a publicly available software maintainability dataset from the Zenodo repository, developed by Hadeel Alsolai , which includes Java-based, class-level data from five different software systems. This research utilizes larger and more up-to-date datasets in various programming languages to enhance the generalization and effectiveness of maintainability prediction models. Feature selection techniques are applied to identify the most relevant metrics, and ensemble models are also considered. Model performance will be evaluated using regression metrics and compared to models from previous studies.

MATERIALS AND METHODS

Research Methodology

This research utilizes a framework that refers to several previous studies and has been modified for the model creation process, which will then be evaluated using various related formulas to measure model performance. The proposed framework in this study is illustrated in Figure 1. Each generated model is obtained from the implementation of the 10-fold cross-validation technique, thus undergoing generalization capability checks.

Dataset

The datasets that used in this study is shown in Table 1. The dataset has 17 independent features. These features are shown in Table 2.

Table 1
Dataset

Datasets	Number of Class
Eclipse JDT Core	695
Eclipse PDE UI	1209
Equinox Framework	276
Lucene	539
Mylyn	1537

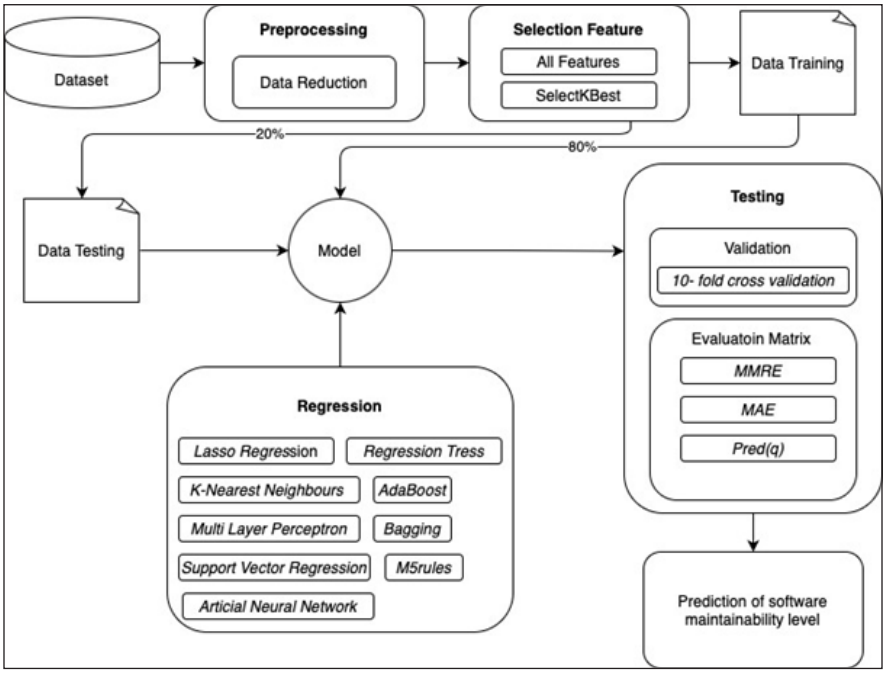

Figure 1. Purpose method

Table 2
Metrics on the software maintainability prediction dataset

Lack of Cohesion in Methods (LCOM)	**Number of Children (NOC)**	**Depth of Inheritance Tree (DIT)**	**Coupling Between Objects (CBO)**	**Response for Class (RFC)**	**Weighted Method Count (WMC)**
FanIn	FanOut	Number of Attributes (NOA)	Number of Attributes Inherited (NOAI)	Lines of Code (LOC)	Number of Methods (NOM)
Number of Methods Inherited (NOMI)	Number of Private Attributes (NOPRA)	Number of Private Methods (NOPRM)	Number of Public Attributes (NOPA)	Number of Public Methods (NOPM)	

Evaluation Metrics

The evaluation metrics used include MMRE, MAE, and Pred. Each metric plays a crucial role in addressing regression problems. This study uses several accuracy measurements for the predictive model, as shown in Table 3. The more precise the prediction model created, while utilizing MMRE and MAE measurements, the smaller the resultant value. (Kumar et al., 2019). Meanwhile, the prediction model generated for Pred(q) data is more accurate the higher the obtained value. (Koten & Gray, 2006).

Table 3
Regression evaluation metrics

No	Metrics	Formula	Description
1	Magnitude of Relative Error (MRE)	$MRE_i = \frac{\lvert y_i - \hat{y}_i \rvert}{y_i}$	Using y_i to represent the actual value and $\hat{y}_i$ to represent the predicted value, MRE calculates the absolute difference between the two values, divided by the actual value.
2	Mean Magnitude of Relative Error (MMRE)	$MMRE = \frac{1}{n}\sum_{i=1}^{i=n} MRE_i$	MMRE means the average value of MRE
3	Mean Absolute Error (MAE)	$MAE = \frac{1}{n}\sum_{i=1}^{i=n} \lvert \hat{y}_i - y_i \rvert$	With y_i standing for the actual value and $\hat{y}_i$ for the anticipated value, MAE calculates the mean of the absolute differences between the two values.
4	PRED (Pred(q))	$Pred(q) = \frac{k}{n}$	The Pred function calculates the proportion of a dataset's examples where the MRE is less than or equal to a specified threshold, *q*. In this case, *n* is the total number of instances in the dataset, *k* is the number of instances having an MRE less than or equal to *q*, and *q* is a defined value.

RESULT AND DISCUSSION

Based on Figure 2, it is known that with the implementation of the bagging ensemble method on individual models, the resulting performance does not always improve. There are several algorithms whose performance decreases on certain datasets, such as the RT algorithm on the Lucene dataset and the M5Rules algorithm on the Eclipse JDT Core, Eclipse PDE UI, and Mylyn datasets. However, for some algorithms on certain datasets, such as M5Rules, MLP, ANN, and RT, there is a significant performance improvement. Generally, the SVR algorithm improves performance on all datasets, although not significantly. The ANN algorithm improves performance on four out of five datasets.

Based on Figure 3, it is known that with the implementation of the AdaBoost ensemble method on individual models, the resulting performance does not always improve. The results show that the ANN algorithm has the best performance on almost all datasets compared to other models in terms of the MMRE metric. The best performance was shown on the Lucene dataset with an MMRE of 0.78.

Table 4 shows that feature selection techniques improve the performance of some algorithms and decrease the performance of others. However, in these individual models, the performance improvement is more dominant compared to the performance decline. The result of 12 selection features are CBO, FanIn, FanOut, LCOM, NOA, LOC, NOM, NOPRA, NOPRM, NOPM, RFC and WMC.

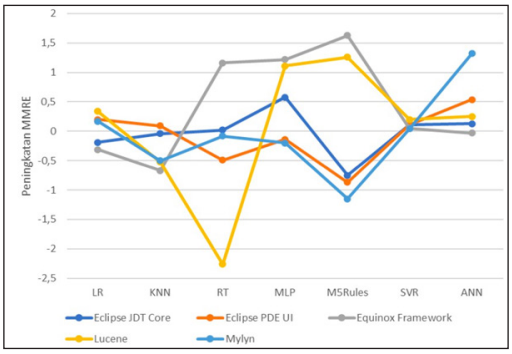

Figure 2. Performance individual model and ensemble bagging model

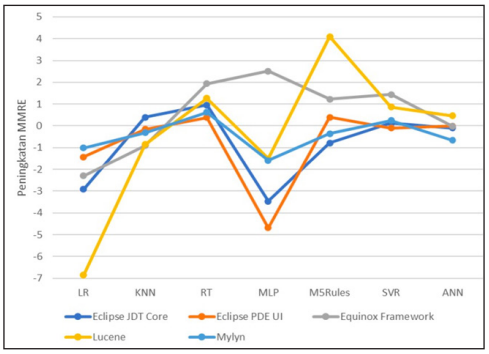

Figure 3. Performance of the individual model and the ensemble adaboost model

Table 4
Performance model with selection feature

Models	**MMRE**				
Lasso Regression	**Eclipse JDT Core**	**Eclipse PDE UI**	**Equinox Framework**	**Lucene**	**Mylyn**
KNN	3.06	4.58	6.86	19.76	4.97
Regression Tree	11.57	3.77	6.63	4.90	4.21
Multilayer Perceptron	2.57	2.28	3.63	4.55	2.45
M5Rules	2.71	2.13	4.81	4.59	3.08
SVM	3.16	2.23	5.61	2.54	1.74
ANN	0.92	0.98	0.88	0.97	0.96

Based on the results obtained by implementing feature selection techniques on the dataset, feature selection techniques can either improve or decrease the performance of machine learning models. The features removed, the algorithm used, data distribution, and data characteristics influence the outcomes of machine learning model creation using feature selection techniques. If the removed features are appropriate and the algorithm used is suitable for the data distribution, then the model's performance will improve. Conversely, if the removed features are not appropriate and the algorithm is unsuitable for the data distribution, then the model's performance will decline.

CONCLUSION

Based on the results obtained by implementing the ensemble method on individual models, it indicates that not all ensemble models improve individual models. Ensemble models can enhance individual models provided that the ensemble method and the individual algorithm used are appropriate, along with good data distribution.

Based on the results obtained by implementing feature selection techniques on the dataset, feature selection techniques can either improve or decrease the performance of machine learning models. The features removed, the algorithm used, data distribution, and data characteristics influence the outcomes of machine learning model creation using feature selection techniques.

ACKNOWLEDGMENT

The author express my deepest gratitude to Universitas Pendidikan Indonesia (UPI) for providing me with the invaluable opportunity to pursue and complete this research. The support and resources provided by UPI have been instrumental in the successful completion of this project.

REFERENCES

Alsolai, H., & Roper, M. (2020). A systematic literature review of machine learning techniques for software maintainability prediction. *Information and Software Technology*, *119*, Article 106214. https://doi.org/10.1016/j.infsof.2019.106214.

Alsolai, H., Roper, M., & Nassar, D. (2018). Predicting software maintainability in object-oriented systems using ensemble techniques. In *2018 IEEE International Conference on Software Maintenance and Evolution (ICSME)* (pp. 716-721). IEEE. https://doi.org/10.1109/ICSME.2018.00088.

Elish, M. O., & Elish, K. O. (2009). Application of treenet in predicting object-oriented software maintainability: A comparative study. In *2009 13th European Conference on Software Maintenance and Reengineering* (pp. 69-78). IEEE. https://doi.org/10.1109/CSMR.2009.57.

Koten, C. V., & Gray, A. R. (2006). An application of Bayesian network for predicting object-oriented software maintainability. *Information and software technology*, *48*(1), 59-67. https://doi.org/10.1016/j.infsof.2005.03.002

Kumar, L., Lal, S., & Murthy, L. B. (2019). Estimation of maintainability parameters for object-oriented software using hybrid neural network and class level metrics. *International Journal of System Assurance Engineering and Management*, *10*(5), 1234-1264. https://doi.org/10.1007/s13198-019-00853-2.

Land, R. (2002). Measurements of software maintainability. In *Proceedings of the 4th ARTES Graduate Student Conference* (pp. 1-7). Atlantis Press.

Thwin, M. M. T., & Quah, T. S. (2005). Application of neural networks for software quality prediction using object-oriented metrics. *Journal of systems and software*, *76*(2), 147-156. https://doi.org/10.1016/j.jss.2004.05.001.

REFEREES
FOR THE
PERTANIKA PROCEEDINGS

Vol. 1 (3) 2025

The Editorial Board of the Pertanika Proceedings wishes to thank the following:

Aslina Saad
UPSI, Malaysia

Aziah Asmawi
UPM, Malaysia

Deden Pradeka
UPI, Indonesia

Emaliana Kasmuri
UTeM, Malaysia

Hamidah Ibrahim
UPM, Malaysia

Khairul Azhar Kasmiran
UPM, Malaysia

Mochamad Iqbal Ardimansyah
UPI, Indonesia

Mustafa Man
UMT, Malaysia

Nor Raihan Zulkefly
USIM, Malaysia

Norhayati Mohd Ali
UPM, Malaysia

Novia Indriaty Admodisastro
UPM, Malaysia

Nur Arzilawati Md Yunus
UPM, Malaysia

Pathiah Abdul Samat
UPM, Malaysia

Razali Yaakob
UPM, Malaysia

Rohaya Latip
UPM, Malaysia

Rozlina Mohamed
UMPSA, Malaysia

Rusli Abdullah
UPM, Malaysia

Shireen Muhammad
UNISEL, Malaysia

Siti Munirah Mohd
USIM, Malaysia

Suhaida Abdul Kadir
UPM, Malaysia

Tuty Asmawaty Abdul Kadir
UMPSA, Malaysia

Umar Ali Bukar
MMU, Malaysia

MMU	*– Multimedia University*	*UPM*	*– Universiti Putra Malaysia*
UMPSA	*– Universiti Malaysia Pahang Al-Sultan Abdullah*	*UPSI*	*– Universiti Pendidikan Sultan Idris*
UMT	*– Universiti Malaysia Terengganu*	*USIM*	*– Universiti Sains Islam Malaysia*
UNISEL	*– Universiti Selangor*	*UTeM*	*– Universiti Teknikal Malaysia Melaka*
UPI	*– Universitas Pendidikan Indonesia*		

While every effort has been made to include a complete list of referees for the period stated above, however if any name(s) have been omitted unintentionally or spelt incorrectly, please notify the Chief Executive Editor, *Pertanika* Journals at executive_editor.pertanika@upm.edu.my

Pertanika Proceedings
Vol. 1 (3) 2025

Content

Pertanika Editorial Office, Journal Division,
Putra Science Park,
1st Floor, IDEA Tower II,
UPM-MTDC Center,
Universiti Putra Malaysia,
43400 UPM Serdang,
Selangor Darul Ehsan
Malaysia

http://www.pertanika.upm.edu.my
Email: executive_editor.pertanika@upm.edu.my
Tel. No.: +603- 9769 1622

PENERBIT UPM
UNIVERSITI PUTRA MALAYSIA
PRESS

http://penerbit.upm.edu.my
Email: dir.penerbit@upm.edu.my
Tel. No.: +603- 9769 8855

eISSN 3083-9475