International Journal of Applied and Scientific Research (IJASR)
Vol. 4 No. 7, 2026: 399-412

Classification of Privacy Violations in Android Application Permissions Using Decision Tree and RapidMiner: A Cyberlaw Perspective

Hafiz Rahmad Putra[1], Guntur Arya Suta[2], Dani Izzudiin[3], Amalya Patria Ika[4], Besus Maulana Sulthon[5]
Universitas Bina Sarana Informatika
Corresponding Author: Besus Maulana Sulthon maulasyarif@gmail.com

A R T I C L E I N F O

Keywords: Android, Decision Tree, Data Privacy, Permission Analysis, UU PDP, Cyberlaw

Received : 27, May
Revised : 28, June
Accepted: 30, July

A B S T R A C T

The rapid growth of Android-based mobile applications in the travel and tourism sector has significantly increased the volume of personal data processed, raising critical concerns regarding privacy violations and over-privileged application behavior. This research aims to classify privacy violations in Android travel application permissions by integrating computational data mining and normative juridical analysis. Using a dataset of 28,771 AndroidManifest.xml metadata files, the Decision Tree algorithm was implemented through the RapidMiner platform using 10-Fold Cross Validation. The experimental results achieved an accuracy of 67.55%, indicating that modern malware often mimics the permission patterns of legitimate applications, making static classification challenging. Extracted decision rules revealed specific "Stealth Malware" patterns and aggressive tracking combinations that bypass standard user awareness. From a cyberlaw perspective, these findings indicate that current permission-based consent mechanisms are insufficient and often conflict with the principles of data minimization and purpose limitation mandated by Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) and the Electronic Information and Transactions Law (UU ITE). This study concludes that permission-based static analysis is no longer a standalone solution, advocating for dynamic security auditing to ensure compliance with Indonesian digital privacy regulations.

DOI: https://doi.org/10.59890/ijasr.v4i7.260
E-ISSN: 3025-7670
https://nvlmultitechpublisher.my.id/index.php/ijasr/ind

INTRODUCTION

The rapid development of digital technology has significantly increased the use of mobile applications across various sectors, including travel and tourism services. Android-based travel applications have become an essential tool for users to book transportation tickets, reserve hotel accommodations, navigate destinations, and conduct digital payment transactions conveniently. This convenience has contributed to the widespread adoption of travel applications while simultaneously leading to the collection of substantial amounts of users' personal data, including location information, personal identities, contact lists, camera access, and device storage. Despite these advantages, such conditions also raise concerns regarding privacy violations when application permissions are requested excessively or beyond the functional requirements of the services provided (Zakariya & Ramli, 2023).

Privacy violations in travel applications have become a significant concern because many applications request access to users' sensitive information. Some applications are even categorized as **over-privileged applications**, referring to applications that request permissions unrelated to their primary functions. For example, a ticket-booking application may request access to users' private messages, contact lists, or microphones without a clear operational justification. Such misuse of application permissions may facilitate unauthorized data collection, digital activity tracking, and theft of personal information. These practices constitute a form of cybercrime that can cause both financial and non-financial harm to users (Zildan, 2025). Previous studies have demonstrated that specific permission patterns exhibit a strong correlation with malicious Android applications and malware, making them valuable indicators for the early classification of application security risks (Aziz et al., 2025).

From the perspective of cyberlaw, the protection of personal data processed by travel applications is regulated under **Law Number 27 of 2022 concerning Personal Data Protection (PDP Law)** and the **Law on Electronic Information and Transactions (ITE Law)**. These regulations emphasize that application developers are required to implement the principle of data minimization by requesting only the permissions necessary for the intended purposes of personal data processing. However, in practice, many users grant requested permissions without fully understanding the potential privacy risks involved. Therefore, an effective method is required to identify and classify potential privacy violations associated with permission requests in travel applications (Syahputra, 2025).

One promising approach is static analysis of the **AndroidManifest.xml** file using data mining techniques. Static analysis enables permission identification without executing the application, making it a more efficient approach for detecting suspicious access patterns. In this study, the **Decision Tree** algorithm was selected because it provides accurate classification results while generating interpretable decision rules in the form of **IF–THEN** logic. This characteristic is particularly relevant within the cyberlaw context because the resulting classification rules are transparent, explainable, and legally accountable. Furthermore, permission-based static analysis has been proven

effective in identifying Android applications that potentially contain malware or pose privacy risks (Wiyono et al., 2025).

To support data processing and model evaluation, this research employs **RapidMiner** as the primary data mining platform. RapidMiner was selected because it provides comprehensive features for data preprocessing, machine learning model development, validation, and performance evaluation in a systematic manner. Model performance is evaluated using a **Confusion Matrix**, with accuracy, precision, and recall serving as the primary evaluation metrics to assess the algorithm's ability to distinguish between secure travel applications and those that potentially violate user privacy. Moreover, the Decision Tree algorithm generates interpretable **IF–THEN** decision rules, making it highly suitable for permission-based classification of Android applications (Budiana & Shelviani, 2025). The implementation of Decision Tree through RapidMiner also facilitates a structured and efficient modeling and evaluation process (Ameliatus & Fatah, 2024; Siahaan, 2025).

Although numerous studies have applied machine learning techniques to detect Android malware based on application permission patterns, most have primarily focused on improving classification accuracy from a technical perspective without relating detection results to privacy violations or their legal implications. Aziz et al. (2025), for example, employed the **XGBoost** algorithm for Android malware classification, while Budiana and Shelviani (2025) combined **Decision Tree** and **Naïve Bayes** to improve malware detection performance. Meanwhile, Zakariya and Ramli (2023) concentrated on assessing privacy risks in mobile applications using machine learning approaches. Nevertheless, studies specifically examining permission patterns in travel applications while integrating classification outcomes with cyberlaw perspectives and compliance with the Personal Data Protection Law remain limited. This condition highlights a significant research gap that warrants further investigation.

Based on these circumstances, this study offers a novel contribution by integrating permission-based classification of Android travel applications using the **Decision Tree** algorithm implemented in RapidMiner with a cyberlaw analysis framework. The novelty of this research lies not only in identifying applications that potentially violate user privacy but also in interpreting the generated **IF–THEN** decision rules as a basis for evaluating developers' compliance with the principles of data minimization and purpose limitation stipulated in the Personal Data Protection Law.

This research is expected to contribute both theoretically and practically. From a theoretical perspective, it enriches the literature on the application of the Decision Tree algorithm for privacy risk analysis of Android applications based on requested permissions. Practically, the findings are expected to serve as a reference for users in understanding the privacy risks associated with granting application permissions, for developers in implementing **privacy by design** principles during application development, and for regulators and legal practitioners in evaluating compliance with Indonesia's personal data protection regulations.

Based on these issues, this study aims to implement RapidMiner and the Decision Tree algorithm to classify privacy violations associated with permission requests in Android-based travel applications from a cyberlaw perspective. The study is expected to contribute to improving awareness of personal data security among travel application users while providing a legal evaluation framework for developers' data management practices in the digital era.

LITERATURE REVIEW

Android is an open-source operating system widely used in mobile devices because it provides developers with flexibility to create applications for various purposes, including communication, education, healthcare, banking, and travel services. Every application requires access to specific device resources to perform its intended functions, such as the camera, location services, microphone, contacts, and storage. Therefore, Android implements a permission mechanism as an access control system designed to protect device security and users' personal data from unauthorized use (Akbar et al., 2022).

Android permissions are categorized into two main types: **Normal Permissions** and **Dangerous Permissions**. Normal Permissions involve low-risk access and are automatically granted by the operating system. In contrast, Dangerous Permissions provide access to sensitive user information and therefore require explicit user consent. Permission misuse commonly occurs when an application requests access rights that are unrelated to its primary functionality, a condition known as an **over-privileged application**, which increases the risk of personal data theft and malware-related activities (Ehsan et al., 2022).

Data mining is the process of extracting valuable information, patterns, and knowledge from large datasets using statistical techniques, artificial intelligence, and computational methods. In the field of cybersecurity, data mining has become an effective approach because it can automatically process large volumes of data to identify characteristics that are difficult to detect through manual analysis. As the number of Android applications available through various distribution platforms continues to increase, data mining provides an efficient solution for identifying applications that are either safe or potentially harmful to users' privacy (Gundla & Gengaje, 2024).

In Android security research, data mining utilizes various application attributes, including permissions, API calls, file size, and other metadata, to develop classification models. Among these attributes, permissions have become one of the most frequently used features because they reflect an application's behavior toward the operating system and user data. Through classification techniques, relationships between permission combinations and application categories can be identified, thereby supporting the early detection of potential privacy violations and malware with greater speed and accuracy (Shakya & Dave, 2022).

Machine learning is a branch of Artificial Intelligence (AI) that enables computers to learn patterns from datasets without being explicitly programmed for every possible condition. Machine learning algorithms utilize historical data

as the basis for learning, allowing them to perform prediction and classification tasks on new data. In cybersecurity, machine learning is widely employed to detect suspicious activities because of its ability to process large volumes of data efficiently (Haq & Khuthaylah, 2024).

In Android application security analysis, machine learning is used to identify application characteristics based on attributes such as permissions, API calls, and other metadata. Models trained using labeled datasets can subsequently classify applications automatically into benign or malware categories. Compared with signature-based detection methods, this approach is considered more adaptive because it is capable of identifying previously unseen patterns (Ansori et al., 2024).

Decision Tree is one of the most widely used classification algorithms in supervised learning. It constructs a hierarchical decision structure by selecting attributes that best distinguish among different data classes. The decision tree is generated by selecting attributes using measures such as **Information Gain** or **Gain Ratio**, enabling each branch to produce increasingly specific decisions until a final class is reached. Owing to its interpretability and simplicity, Decision Tree has been extensively applied in data classification studies, including Android application security analysis (Sk & Anu, 2022).

One of the primary advantages of the Decision Tree algorithm is its ability to generate decision rules in the form of **IF–THEN** logic, which can be easily interpreted by both researchers and end users. This characteristic allows the algorithm not only to produce classification results but also to explain why a particular instance belongs to a specific category. In Android malware detection research, Decision Tree has demonstrated strong performance in identifying application permission patterns and can serve as a transparent basis for evaluating potential privacy violations (AlJarrah et al., 2022).

RapidMiner is a software platform widely used for data mining and machine learning because it provides a graphical user interface (GUI) that enables users to develop analytical models without requiring complex programming. Data processing is conducted through a workflow-based approach, allowing stages such as data import, preprocessing, attribute transformation, model development, and evaluation to be integrated within a single working environment. This approach makes RapidMiner an effective platform for implementing classification algorithms, including Decision Tree (Ameliatus & Fatah, 2024).

In addition to providing various classification algorithms, RapidMiner includes evaluation operators such as **Split Validation**, **Cross Validation**, and **Performance**, which are used to assess model quality using metrics such as accuracy, precision, recall, and the confusion matrix. When implementing the Decision Tree algorithm, RapidMiner also generates visual representations of the decision tree, enabling classification rules to be interpreted in the form of **IF–THEN** logic. These capabilities facilitate researchers' understanding of the decision-making process while supporting systematic evaluation of classification performance (Abrori & Fatah, 2024).

The rapid advancement of digital technology has significantly increased the processing of personal data by various applications, including Android applications. This development necessitates regulations that ensure the protection of individuals' privacy rights. In Indonesia, such protection is provided under **Law Number 27 of 2022 concerning Personal Data Protection (PDP Law)**, which establishes the legal framework governing the collection, use, storage, and deletion of personal data while requiring data controllers to process personal data lawfully, transparently, and within clearly defined limitations (Khair & Wiraguna, 2025).

From a cyberlaw perspective, the misuse of Android permissions may constitute a violation of the principles of **purpose limitation** and **data minimization**, particularly when an application requests access to data that is irrelevant to its primary function. In addition to the PDP Law, such practices may also violate the **Electronic Information and Transactions Law (ITE Law)** concerning unauthorized access to electronic systems and electronic information. Consequently, permission classification using the Decision Tree algorithm can serve as a supporting instrument for compliance auditing and the early identification of potential legal violations within the digital environment (Pranindya, 2025).

Research on Android malware detection and privacy violations has advanced considerably through the application of various machine learning techniques. Most studies employ application permissions as the primary feature because every Android application must request access to device resources before execution. Permission pattern analysis has proven effective in identifying applications that potentially engage in malicious activities, particularly when they request permissions unrelated to their intended functionality. Therefore, permissions have become one of the most effective indicators for Android application classification using machine learning algorithms (Ehsan et al., 2022).

Previous studies have also demonstrated that classification algorithms such as **Decision Tree**, **Random Forest**, and **Gradient Boosting Machine** achieve high levels of accuracy in permission-based Android malware detection. However, the majority of these studies primarily focus on improving model performance through feature optimization and accuracy evaluation without linking classification outcomes to personal data protection or legal compliance. As a result, their findings generally remain limited to technical aspects and have not been extensively utilized as supporting instruments for policy analysis or digital compliance auditing (Turnip et al., 2023).

Based on the review of previous studies, a significant research gap has been identified. Existing research generally focuses on classifying Android applications into benign and malware categories based on permission patterns. In contrast, this study not only applies the Decision Tree algorithm using RapidMiner but also integrates the classification results with a cyberlaw perspective, particularly regarding the implementation of **Law Number 27 of 2022 concerning Personal Data Protection**. Accordingly, the resulting **IF–THEN** classification rules are expected to provide a foundation for analyzing potential

privacy violations and supporting legal compliance audits of Android applications.

METHODOLOGY

This study was conducted systematically using a multidisciplinary approach that integrates a computational experimental method (data mining) with a normative juridical analysis. The research process began with the identification of issues related to Android application permissions, followed by dataset collection from the **AndroidManifest.xml** file, data preprocessing, and classification modeling using the **Decision Tree** algorithm implemented in **RapidMiner**. The decision rules generated by the computational model were subsequently extracted and analyzed from the perspective of Indonesian cyberlaw to provide a comprehensive interpretation of the findings. The overall research methodology is illustrated in the flowchart presented in **Figure 1**.

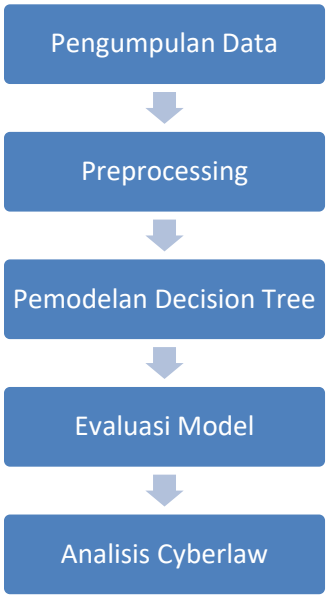

Figure 1. Research Methodology Flowchart

The dataset used in this study consists of secondary data in the form of permission metadata extracted from the **AndroidManifest.xml** configuration files of Android applications. The dataset was obtained from the public **Kaggle** repository and comprises a total sample of **28,771 applications**.
The dataset was represented using two primary components for the classification process:

- **Independent Variables (Features):** These consist of sensitive permission categories declared by the applications, including **Personal Information, Access Location, Access Messages, Access Google Accounts,** and **System Tools**.
- **Dependent Variable (Class Label):** This represents the classification target indicating the potential level of privacy violation. The target variable is categorized into two binary classes: **0 (Benign)**, representing applications considered safe from data misuse, and **1 (Malware)**,

representing applications suspected of unauthorized access and privacy violations.

The data mining process adopted in this study follows a standard analytical framework consisting of the following technical stages:

- **Data Preprocessing:** The raw dataset was initially examined and cleaned by removing duplicate records (**data cleaning**). Subsequently, the data were transformed into a binary matrix (**data transformation**). A value of **1** was assigned when an application explicitly requested a particular permission, whereas a value of **0** indicated that the permission was not requested. This binary transformation was essential for optimizing the computational processing performed by the classification algorithm.
- **Classification Modeling:** The cleaned binary dataset was imported into the **RapidMiner** platform for classification modeling. The **Decision Tree** algorithm was employed to construct the classification model. The tree branching criterion (**split criterion**) was determined using the **Gain Ratio** measure to generate efficient prediction rules with strong generalization capability for unseen data.
- **Model Validation:** To evaluate model stability and reduce the risk of performance bias caused by overfitting, this study employed the **10-Fold Cross-Validation** technique. The dataset was randomly partitioned into ten equal subsets (folds). During each iteration, nine folds were used as the **training set**, while the remaining fold served as the **testing set**. This rotation process was repeated ten times until each fold had been used once as the testing set.

The performance of the **Decision Tree** algorithm in classifying potential privacy violations was quantitatively evaluated using a **Confusion Matrix**. This evaluation is based on four fundamental classification outcomes: **True Positive (TP), True Negative (TN), False Positive (FP),** and **False Negative (FN)**. The performance metrics employed in this study were calculated using the following mathematical equations:

- (Accuracy): Measures the proportion of correctly classified instances, including both positive and negative predictions, relative to the total number of testing instances.
  Accuracy = (TP + TN) / (TP + TN + FP + FN)
- (Precision): Measures the proportion of correctly predicted positive instances among all instances predicted as positive.
  Precision = TP / (TP + FP)
- Recall: Measures the model's ability to correctly identify all actual positive instances, indicating its sensitivity in detecting the target class.
  Recall = TP / (TP + FN)

In the final stage, the **Decision Tree** generated in **RapidMiner** was converted into a set of logical **IF–THEN decision rules**. These rules were used to identify combinations of sensitive application permissions that algorithmically trigger the prediction of **Class 1**, indicating a potential privacy violation.

The resulting classification rules were subsequently analyzed qualitatively using a **normative juridical approach**. Permission patterns identified as potentially

harmful were critically examined in relation to Indonesia's prevailing cyberlaw framework. The analysis focused on the interpretation of **Law Number 27 of 2022 concerning Personal Data Protection (Personal Data Protection Law)**, particularly the principles governing the lawful processing of personal data, as well as the **Electronic Information and Transactions (ITE) Law**, specifically its provisions concerning unauthorized access (**illegal access**). This legal analysis aimed to evaluate the extent to which Android application developers comply with applicable legal requirements governing the collection and processing of users' personal data.

RESULTS AND DISCUSSION

Based on the computational experiment using the **Decision Tree** algorithm with the **10-Fold Cross-Validation** method on the Android application permission dataset, the classification model was evaluated using a **Confusion Matrix** to assess its performance in distinguishing between **Malware (Class 1)** and **Benign (Class 0)** applications. The evaluation results indicate that the proposed classification model achieved an overall **accuracy of 67.55%**.

Table 1. Confusion Matrix Evaluation Results of the Decision Tree Algorithm

	true 0	true 1	class precision
pred. 0	1361	1151	54.18%
pred. 1	8159	18015	68.83%
class recall	14.30%	93.99%	

More specifically, the model achieved a **class precision** of **68.83%** for **Malware (Predicted Class 1)** and **54.18%** for **Benign (Predicted Class 0)**. In terms of sensitivity, the model demonstrated a remarkably high **class recall** of **93.99%** for the Malware class, indicating its strong capability to identify malicious applications. However, the recall for the Benign class remained relatively low at **14.30%**, suggesting that many legitimate applications were incorrectly classified as malware.

The overall accuracy of approximately **67.55%** represents an important empirical finding of this study. This result indicates that the Decision Tree algorithm faces considerable challenges in establishing a clear distinction between malicious and benign applications when relying solely on statically declared application permissions. From a technical perspective, this finding suggests that modern malware developers increasingly design permission request structures that closely resemble those of legitimate Android applications. By requesting permission combinations commonly found in benign applications, malicious software can effectively obscure its true behavior and reduce the effectiveness of static permission-based classification methods.

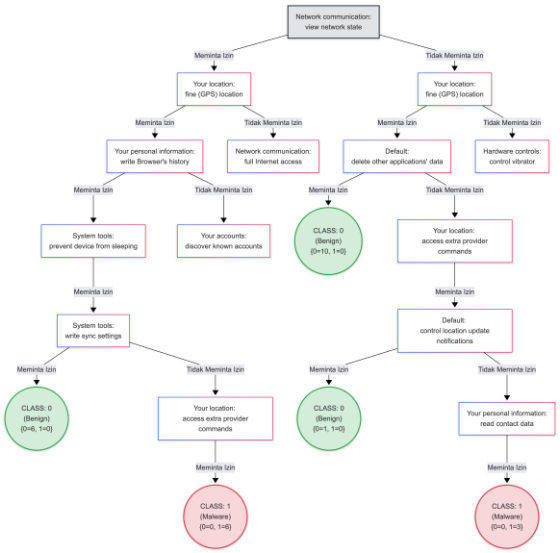

Figure 3. Visualization of the Decision Tree Model in RapidMiner

Based on the modeling results generated using **RapidMiner**, several dominant **decision rules** were extracted that contributed significantly to the classification of applications into the malicious or **Malware** category. The dominant rules are described as follows:

First, the Aggressive Tracking Combination Pattern (Rule 1) indicates that when an application requests permission to view network status, access the user's precise location (**fine/GPS location**), and modify or write browser history and bookmarks, the system classifies the application as **Malware**. This combination of attributes represents a multi-layered privacy violation pattern, in which the application simultaneously monitors network conditions, tracks precise GPS coordinates, and modifies the user's browsing history without legitimate authorization.

Second, the Stealth Malware Application Anomaly Pattern (Rule 2) identifies a manipulative profile in which an application that does not request permission to view network status, requests at most one dangerous permission, and does not request any safe permission is still classified as **Malware**. This pattern reveals a highly concerning anomaly because malicious developers intentionally manipulate application architectures by requesting very limited permissions (or even no safe permissions at all) to create the appearance of harmlessness and avoid user suspicion during installation. This rule represents a significant finding, as it successfully classified more than **4,900 malware samples** within the dataset.

The extraction of these decision rules from the computational model provides a strong empirical foundation for further analysis from an Indonesian cyberlaw perspective, particularly in relation to the **Personal Data Protection Law (PDP Law)** and the **Electronic Information and Transactions Law (ITE Law)**.

First, the findings from **Rule 1** highlight significant weaknesses in the mechanism of user consent. **Article 22 of the PDP Law** stipulates that consent for personal data processing must be obtained lawfully, explicitly, and transparently

in accordance with the intended purpose of processing. However, the combination of GPS location tracking and browser history modification is often embedded in applications whose primary functions do not require such data access, such as utility applications or games. This condition causes the consent provided by users during installation to become legally questionable in substance because users are misled regarding the actual purpose of data processing.

Second, the **Stealth Malware phenomenon** identified in **Rule 2** is highly relevant to cybercrime indicators under the **ITE Law**. Applications that appear not to declare standard access permissions but secretly operate as malware in the background may fulfill the elements of **Article 30 of the ITE Law** concerning unauthorized access (**illegal access**). Application developers may intentionally design software architectures that manipulate Android system interfaces and conceal data exploitation activities from user supervision.

This study concludes that static Android permission declarations can no longer be relied upon as the sole mechanism for protecting user privacy. From a computational perspective, the Decision Tree accuracy of **67.55%** demonstrates a substantial similarity between permission patterns of malicious and legitimate applications, indicating the need for more comprehensive security analysis approaches. From a cyberlaw perspective, the exploitation of seemingly normal permission features undermines the principles of transparency and purpose limitation established under the PDP Law while simultaneously fulfilling the characteristics of illegal access as regulated under the ITE Law.

CONCLUSION AND RECOMMENDATION

This study concludes that the implementation of data mining using the **Decision Tree** algorithm through the **RapidMiner** platform is effective in identifying critical permission combinations or **dangerous permissions** in Android applications. Although the static classification evaluation achieved an accuracy rate of **67.55%**, this metric empirically demonstrates the high similarity between the permission profiles of modern malware and legitimate (**benign**) applications. The algorithm successfully extracted logical **IF–THEN decision rules** that accurately revealed the presence of **over-privileged application** threats, particularly through aggressive tracking patterns and stealth malware application anomalies.

From a **cyberlaw perspective**, the technical findings confirm that static permission-based consent mechanisms are no longer sufficient as the sole instrument for protecting user privacy. Excessive permission manipulation practices have substantially undermined the principles of transparency, data minimization, and purpose limitation mandated by **Law Number 27 of 2022 concerning Personal Data Protection (PDP Law)**. Furthermore, hidden (**stealth**) activities intended to exploit user data may fulfill the legal elements of **illegal access** offenses within the framework of the **Electronic Information and Transactions Law (ITE Law)**.

This research successfully bridges the gap identified in previous studies by demonstrating that machine learning model outputs can be transformed into

legitimate legal-support instruments for compliance auditing and the standardization of digital forensic evidence. For future research, it is recommended that security analysis should not rely solely on static examination of the **AndroidManifest.xml** file but should also incorporate **dynamic analysis** through sandbox-based testing environments. This approach is necessary to monitor actual data flows (**real-time data traffic**) and **API calls** in order to overcome the limitations of static classification accuracy.

Furthermore, future studies may expand comparative classification approaches by implementing **deep learning** or **ensemble learning** methods, as well as developing an automated security auditing framework that is directly integrated with compliance parameters based on Indonesia's **Personal Data Protection Law (PDP Law)** standards.

REFERENCE

Abrori, S., & Fatah, Z. (2024). Implementasi Metode Decision Tree Dalam Mengklasifikasi Depresi Menggunakan Rapidminer. Journal of Students' Research in Computer Science, 5(2), 123–132. https://doi.org/10.31599/vgf7xb32

Akbar, F., Hussain, M., Mumtaz, R., Riaz, Q., Wahab, A. W. A., & Jung, K. H. (2022). Permissions-Based Detection of Android Malware Using Machine Learning. Symmetry, 14(4). https://doi.org/10.3390/sym14040718

AlJarrah, M. N., Yaseen, Q. M., & Mustafa, A. M. (2022). A Context-Aware Android Malware Detection Approach Using Machine Learning. Information (Switzerland), 13(12), 1–25. https://doi.org/10.3390/info13120563

Ameliatus, Q., & Fatah, Z. (2024). Klasifikasi Kelulusan Mahasiswa Menggunakan Decision Tree. Jurnal Riset Teknik Komputer, 1(4), 58–64. https://journal.smartpublisher.id/index.php/jurtikom/article/view/305

Ansori, D. B., Slamet, J., Ghufron, M. Z., Putra, M. A. R., & Ahmad, T. (2024). Android Malware Classification Using Gain Ratio and Ensembled Machine Learning. International Journal of Safety and Security Engineering, 14(1), 259–266. https://doi.org/10.18280/ijsse.140126

Aziz, T. A., Sari, Z., Sri, C., & Aditiya, K. (2025). Klasifikasi Malware Android dengan menggunakan metode XGBoost Algoritma. Repositor, 7(1), 103–110.

Budiana, F. P., & Shelviani, H. (2025). Kombinasi Algoritma Decision Tree dan Naive Bayes untuk Meningkatkan Akurasi dan Kecepatan Waktu Deteksi Malware. Semnas Ristek (Seminar Nasional Riset Dan Inovasi Teknologi), 9(1), 419–425. https://doi.org/10.30998/semnasristek.v9i1.7874

Ehsan, A., Catal, C., & Mishra, A. (2022). Detecting Malware by Analyzing App Permissions on Android Platform: A Systematic Literature Review. Sensors, 22(20). https://doi.org/10.3390/s22207928

Gundla, R., & Gengaje, S. R. (2024). Android Malware Detection Using Machine Learning. Lecture Notes in Networks and Systems, 1005 LNNS, 47–54. https://doi.org/10.1007/978-981-97-4928-7_4

Haq, M. A., & Khuthaylah, M. (2024). Leveraging Machine Learning for Android Malware Analysis: Insights from Static and Dynamic Techniques. Engineering, Technology and Applied Science Research, 14(4), 15027–15032. https://doi.org/10.48084/etasr.7632

Khair, F., & Wiraguna, S. A. (2025). Data Protection Impact Assessment (DPIA) sebagai Instrumen Kunci Menjamin Kepatuhan UU PDP 2022 di Indonesia. Politika Progresif : Jurnal Hukum, Politik Dan Humaniora, 2(2), 246–254. https://doi.org/10.62383/progres.v2i2.1821

Pranindya, K. R. A. (2025). Penegakan Hukum terhadap Pelaku Penyalahgunaan Penyebaran Data Pribadi Melalui Barcode Ditinjau dari UU ITE dan UU Nomor 27 Tahun 2022 Tentang (UU PDP). Konsensus : Jurnal Ilmu Pertahanan, Hukum Dan Ilmu Komunikasi, 2(3), 123–135. https://doi.org/10.62383/konsensus.v2i3.957

Shakya, S., & Dave, M. (2022). Analysis, Detection, and Classification of Android Malware using System Calls. ArXiv Preprint ArXiv:2208.06130. http://arxiv.org/abs/2208.06130

Siahaan, D. (2025). Math Unesa. Jurnal Ilmiah Matematika, 13(2), 198–199.

Sk, H. K., & Anu, V. M. (2022). A Hybrid Model for Android Malware Detection using Decision Tree and KNN. International Journal on Recent and Innovation Trends in Computing and Communication, 10(November), 321–328. https://doi.org/10.17762/ijritcc.v10i1s.5899

Syahputra, M. D. (2025). Dinamika Hukum Pidana Dalam Menanggapi Kejahatan Siber Di Era Digital. Jurnal Ilmiah Multidisiplin Terpadu, 9(5), 2246–6111.

Turnip, T. N., Manurung, C. F., Lubis, Y. S., & Gulton, R. (2023). Classification of Android Application Malware Using Random Forest Based on Static Features. Jurnal Teknik Informatika Dan Sistem Informasi, 10(1), 926–936.

Wiyono, T., Hadinata, E., Zakir, A., & Elhanafi, A. M. (2025). Deteksi Malware Berbasiskan Analisis Statis Menggunakan Algoritma Convolutional Neural Network (CNN). Jurnal Sistem Komputer Dan Informatika (JSON), 104(1), 94–104.

Zakariya, R. A. I., & Ramli, K. (2023). Desain Penilaian Risiko Privasi Pada Aplikasi Seluler Melalui Model Machine Learning Berbasis Ensemble

Learning. Jurnal Teknologi Informasi Dan Ilmu Komputer, 10(4). https://doi.org/10.25126/jtiik

Zildan, M. (2025). Penggunaan Algoritma Random Forest Untuk Deteksi Malware Berdasarkan Pola Permission Pada Aplikasi Android Komunikasi. Jurnal Cakrawala Informasi, 5(1), 30–49. https://doi.org/10.54066/jci.v5i1.559