International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Machine Learning-Based Risk Classification of Cybersecurity Behavior Among Smartphone Users

Marc Jordan C. Saladaga

Instructor I, JH Cerilles State College

Abstract

Smartphone users today face an increasingly complex landscape of cybersecurity threats, many of which arise not from technical flaws but from behavioral vulnerabilities such as weak password practices, reliance on unsecured public Wi-Fi, and indiscriminate application downloads. These human-centered risks underscore the importance of developing frameworks that can systematically analyze user behavior and provide actionable insights to strengthen digital safety. Addressing this need, our study introduces a machine learning–based approach that integrates behavioral analysis with interpretable models to classify users according to their risk levels.

To build this framework, we collected and preprocessed survey data from 2,751 respondents, ensuring representativeness and reliability of behavioral features. Three machine learning models—Gradient Boosting, Random Forest, and Logistic Regression—were trained and evaluated for performance. Gradient Boosting emerged as the most effective, achieving an overall accuracy of 0.74 and demonstrating superior recall in detecting high-risk users. This balanced performance highlights its potential as a practical tool for identifying vulnerable individuals and guiding targeted interventions.

Beyond predictive accuracy, the framework emphasizes transparency through Explainable AI techniques such as SHAP and LIME, which reveal the behavioral factors most influential in risk classification. These interpretability tools not only validate the model's outputs but also provide meaningful guidance for users and institutions seeking to mitigate vulnerabilities. By combining behavioral analysis with interpretable machine learning, this study contributes both a methodological advancement and a practical solution for delivering customized cybersecurity awareness, ultimately fostering a culture of proactive digital safety among smartphone users.

Keywords: Cybersecurity, Smartphone Users, Machine Learning, Gradient Boosting, Risk Classification, SHAP, LIME, Behavioral Analysis, Explainable AI, Awareness Modeling

1. Introduction

With smartphones becoming people's first choice for communication, financial services, and social interactions [1], security has become a significant issue in the digital era. Smart devices are becoming increasingly vulnerable to cyber threats, including phishing, malware, ransomware, and data theft, which exploit vulnerabilities in user behavior and system design [4]. Although traditional security measures, such

as passwords, antivirus software, and educational campaigns, are still necessary, they are often insufficient in handling advanced attack patterns or meeting the guidelines of changing trends in mobile usage [2].

User consideration and performance have been emphasized in previous work on reducing mobile threats [1]. Weak password management, over-reliance on untrusted apps, and public Wi-Fi networks have been identified as key elements contributing to vulnerability [2]. Literature also emphasizes the importance of machine learning in cybersecurity, where algorithms are used to identify anomalies, classify the degree of risk, and forecast potential threats [6]. These are promising approaches; however, many are still centralized on a generalized system, rather than being personalized for different kinds of users [7].

Despite these advances, many gaps remain: traditional awareness programs provide guidelines that are typically static and represent only a starting point towards solving the true complexity of user behavior [1], while narrow datasets often restrict machine learning models or lack explainability, making it difficult to translate into actionable, end-user recommendations [6]. Many smartphone users, therefore, remain exposed to cyber risks even in the presence of technical safeguards and awareness campaigns [4].

This paper proposes a machine learning framework that classifies the risk level of smartphone users based on behavioral patterns. It aims to deliver personalized recommendations for avoiding identified vulnerabilities, based on several factors, including password strength, application installation, and network usage habits [5]. The proposed solution differs from others in that it incorporates explainable AI techniques, making it more transparent and usable by allowing users to understand their risk classification and act accordingly [6].

The rest of the paper is structured as follows: Section 2 provides a literature review on related works in the fields of smartphone cybersecurity and machine learning applications; Section 3 describes the methodology and dataset used; Section 4 presents the Results and Discussion [7]. This study contributes to existing literature in three ways: (1) it develops a behavioral risk classification model tailored for smartphone users, (2) it integrates explainable AI into the model to build user trust and comprehension, and (3) it offers personalized cybersecurity recommendations to translate awareness into actionable defense [6]. Few studies have been conducted on behavioral analysis integrated with machine learning for adaptive, user-centered interventions; thus, this research will contribute to extending current knowledge in both academic and practical mobile cybersecurity [3].

2. Literature Review

A. Smartphone Cybersecurity Threats

Hence, in modern society, smartphones have become indispensable for communication, banking, education, and entertainment. However, their extensive usage has simultaneously made them the central target for cyberattacks [8]. Mobile malware, phishing campaigns, and spyware have continued to increase globally, with a record of more than 33.8 million mobile attacks this year, 2023 [9].

Despite all efforts, phishing remains one of the most common threats that manipulate users through fake SMS messages, emails, and social media links. Research indicates that mobile phishing campaigns are increasingly targeting enterprises, and most employees tend to fall victim due to the smaller screen sizes and limited security cues [10]. Malware, including trojans and ransomware, continues to infect smartphones via malicious applications, particularly in the open ecosystem of Android, where it is common to sideload apps [9].

User behavior significantly contributes to vulnerability. Poor password practices, frequent installation of unverified apps, and reliance on unsecured public Wi-Fi networks increase the level of exposure [12]. Studies have shown that most people are unaware of mobile threats as compared to a desktop environment, leading to poor adoption of protection measures [9].

Cybersecurity awareness programs have been implemented to mitigate such risks, but evidence suggests that generalized guidelines fail to capture the diverse and dynamic behaviors of smartphone users [14]. As a result, despite the availability of antivirus tools and awareness campaigns, mobile users remain vulnerable to evolving cyber threats.

B. Gaps in Existing Studies

Although some previous work has researched cybersecurity threats through smartphones and user awareness, most studies have stopped at questionnaires and generalized guidelines [1]. While these surveys provide valuable baseline insights, they often fail to capture the complexity of real-world user interactions with mobile devices, leaving a gap in practical risk assessment [2]. For instance, phishing and malware attacks continue to evolve in sophistication, exploiting human factors and mobile-specific vulnerabilities that are not adequately addressed by static awareness campaigns [2][4].

Machine learning models have indeed been applied to mobile security; however, many of these approaches rely on narrow datasets, focus on signature-based detection, or lack explainability, thereby limiting their utility for end-users and practitioners [5][13]. Recent studies highlight that gradient boosting and deep learning models can improve detection accuracy, but without transparent reasoning, users and administrators struggle to trust and adopt these systems [13]15][16].

Thus, there remains a pressing need for frameworks that integrate behavioral analysis with transparent machine learning methods to deliver personalized, actionable recommendations 6][11]. Explainable AI approaches, such as SHAP and LIME, have shown promise in bridging this gap by making model predictions interpretable, which is critical for risk classification in cybersecurity contexts [16][17]. Combining behavioral biometrics, psychometric evaluation of user actions, and interpretable ML can create robust, user-centered defenses that go beyond traditional awareness programs [7]11][12].

3. Methods

This section describes the research design and the technical methodology followed in constructing a machine learning framework that classifies the cybersecurity risk levels of smartphone users. This methodology is presented in a manner that makes it reproducible and easy to follow. It begins by describing the procedures followed during data collection, followed by the identification of behavioral features related to mobile security. Next, the various machine learning models employed for risk classification are presented, along with the metrics used for evaluating their performance. Finally, the integration of explainable AI techniques is discussed to highlight how transparency and interpretability are achieved in the proposed framework.

A. Research Design

This study employs a quantitative descriptive research design, chosen for its ability to capture measurable aspects of smartphone user behavior systematically. Data collection is facilitated through a structured survey administered via Google Forms, ensuring accessibility and ease of distribution across diverse respondents. A non-probability sampling technique was adopted, which, although not guaranteeing full representativeness, allows for the practical recruitment of participants and the efficient gathering of insights into standard practices.

The survey instrument was designed to elicit information on critical security behaviors, including password management strategies, sources of mobile application installation, and reliance on public Wi-Fi networks. These variables were selected because they represent high-risk areas that are frequently exploited in mobile cybersecurity incidents.

The descriptive approach enables the identification of recurring patterns, frequencies, and variations in user practices, providing a baseline understanding of behavioral trends. Meanwhile, the quantitative orientation enables the statistical analysis of risk factors, such as correlations between unsafe practices and demographic characteristics, thereby providing evidence-based insights into vulnerabilities. This methodological framework ensures that findings are not only descriptive but also analytically grounded, supporting the development of targeted awareness programs and risk-mitigation strategies. The collected data are then prepared for machine learning classification to complement the survey, with behavioral features as input variables for predicting risk levels. This hybrid design ensures that the combination of survey-based data collection and computational modeling is both empirically sound and technically rigorous, thereby addressing the research objectives.

B. Data Collection

Data for this study were collected through a structured survey administered via Google Forms. The questionnaire was designed to capture the cybersecurity behaviors of smartphone users, including password practices, the frequency of app installations from unverified sources, and reliance on public Wi-Fi networks. The respondents were recruited by purposive sampling, targeting those who use smartphones for active communication, financial transactions, and online services.

Data for this study were collected using a structured survey via Google Forms, which allowed for the capture of patterns regarding password management, app installation source types, and the use of public Wi-Fi among smartphone users. The survey consisted of closed-ended and Likert-scale questions to quantify behavioral patterns. At the same time, demographic information, including age, gender, and educational background, was solicited to analyze the variations across user groups.

In all, 2,751 respondents participated in the study across both survey batches. The majority were aged between 18 and 34 years old, with 56.2% aged 18–24 and 25.3% aged 25–34 in the second batch. Meanwhile, the first batch consisted of 76.3% of participants who fell within the 25–34 age range. Overall, the gender distribution was relatively balanced, with the first batch comprising 73.2% females and 25.7% males, while the second batch consisted of 50.5% males and 49.5% females.

Regarding occupation, students were the most dominant group in both sets, at 87.2% and 56.2%, respectively, while others were employed, teachers, or self-employed. In terms of smartphone usage, 67.6% of the first batch reported using their devices for more than four hours daily, while 56.2% of the second batch reported constant use. Device preference leaned heavily toward Android smartphones at 89.7% in the first batch and 56.2% in the second. The app download behavior showed strong adherence to official sources, with 89.9% of the first batch and 81.5% of the second batch using Google Play or the Apple App Store.

Additional behavioral indicators obtained from a subsample of younger respondents (LPS group) showed that 100% used YouTube, followed by Instagram (83.3%) and TikTok (75%). Most contacted age peers online daily, 58.3%, while 75% rarely or never connected to public Wi-Fi. Regarding the scam awareness question, only 16.7% felt very confident in their ability to recognize online scams, while 50% ranked themselves as moderately or not very confident at all. In self-assessed cybersecurity risk levels, 41.7% identified themselves as low risk, 33.3% as moderate, and 25% as high or very high risk.

These demographics and behavioral patterns indicate a predominantly young, student-based population with high smartphone engagement and varied cybersecurity practices, making them highly relevant for modeling risk classification and awareness.

To guarantee data integrity, answers were anonymized and securely stored. This dataset was then preprocessed, cleaning incomplete entries and standardizing them for input into machine learning models, ensuring that the collected data was reliable and suitable for further risk classification.

C. Feature Selection / Behavioral Factors

The features chosen for this research were selected based on survey response variables that best describe the typical cybersecurity behavior of smartphone users. The most relevant features involved the type of screen lock in use: none, simple PIN/password, complex PIN/password, pattern, biometric, or combined, which shows baseline device access protection. Application downloading behavior also fell into one of two categories: using only official app stores or occasionally/frequently using third-party sources.

Other features include the use of mobile security tools, such as antivirus apps, VPNs, app permission managers, and two-factor authentication. All these variables were encoded as binary indicators to represent the presence or absence of protective measures. Device type, such as Android, iOS, basic phone, and frequency of smartphone use, was also included to put the level of exposure into context. These collectively form an input set for machine learning-based risk classification, enabling it to identify patterns associated with low, moderate, and high cybersecurity risk profiles.

D. Machine Learning Model

In the context of the present study, the selected machine learning model is Gradient Boosting, an ensemble technique that incrementally builds multiple weak learners, typically decision trees, in sequence. Each successive tree is trained to correct the errors of its predecessor, enabling the model to capture complex, nonlinear relationships within the dataset. This iterative refinement makes Gradient Boosting significantly more accurate and robust than baseline models, such as Logistic Regression or single Decision Trees, which often struggle with high-dimensional behavioral data [19][20].

The dataset, collected through Google Form surveys, encompasses both demographic and behavioral variables, including age range, occupation, sources of mobile application installation, screen lock usage, and frequency of public Wi-Fi connections. These features are directly linked to smartphone security practices and provide a rich basis for risk classification. Gradient Boosting is particularly well-suited for such tabular data, as it can seamlessly integrate categorical and numerical variables while ranking the most influential predictors of cybersecurity risk.

Recent implementations, such as XGBoost, LightGBM, and CatBoost, extend the classical Gradient Boosting framework by introducing optimized algorithms that facilitate faster training, reduced memory consumption, and improved scalability on large datasets [21]. These libraries also incorporate regularization techniques to prevent overfitting, making them practical for real-world applications where data quality and volume vary.

Equally important is the model's interpretability. Transparency tools, such as SHAP (SHapley Additive exPlanations), provide user-friendly explanations of how predictions are made [22]. For example, SHAP values can highlight whether frequent use of public Wi-Fi or downloading apps from unofficial sources contributes most to a user's classification as Low, Moderate, or High risk. This interpretability ensures that the model's outputs are not only statistically valid but also actionable for end-users and policymakers.

Taken together, the evaluation criteria of accuracy, scalability, and interpretability position Gradient Boosting as a highly suitable choice for this research. It balances predictive performance with transparency, thereby supporting the development of a practical framework for cybersecurity risk classification that is both technically rigorous and user-centered.

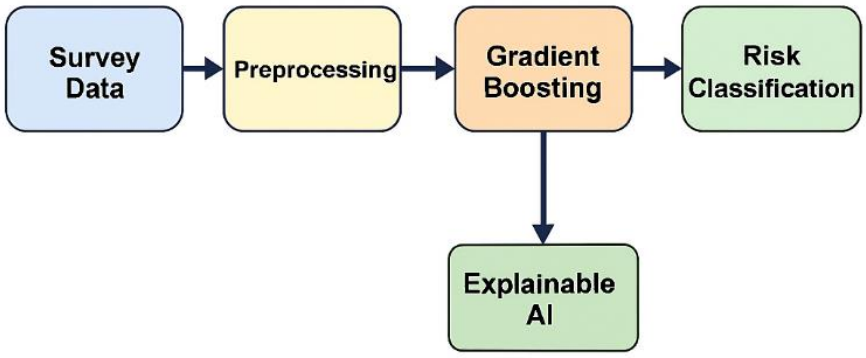

Figure 1. Workflow of the proposed machine learning risk classification framework.

E. Explainable AI Integration

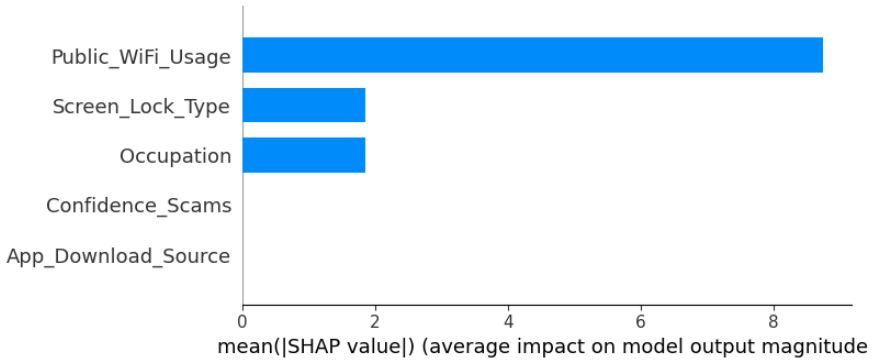

Figure 2. SHAP Feature Importance for Risk Classification

This work incorporates Explainable Artificial Intelligence (XAI) tools to enhance the transparency of the Gradient Boosting model. While Gradient Boosting is widely recognized for its strong predictive performance and robustness, it is often criticized as a "black-box" model because its internal decision processes are challenging to interpret. To address this limitation, the study integrates **SHAP (SHapley Additive exPlanations)**, which quantifies the contribution of each feature to the model's output. Through SHAP values, the analysis highlights which behavioral factors—such as frequent use of public Wi-Fi, downloading applications from unofficial sources, or weak screen lock practices—are most influential in classifying users into Low, Moderate, or High-risk **categories** [23].

In addition, LIME (Local Interpretable Model-agnostic Explanations) is employed to provide case-by-case interpretability. LIME approximates the complex Gradient Boosting model with a simpler surrogate model for each prediction, thereby offering localized insights into why a particular user is assigned a specific risk level. This dual approach ensures that the framework delivers both **global interpretability** (overall feature importance across the dataset) and **local interpretability** (explanations for individual predictions).

By combining SHAP and LIME, the study not only achieves high accuracy but also ensures that the model's outputs are **understandable and actionable**. This interpretability is critical for translating technical findings into practical awareness campaigns and digital safety practices, empowering users and organizations to make informed decisions about mobile cybersecurity risks.

4. Result and Discussion

This section presents the outcomes of the machine learning experiments conducted using the Gradient Boosting classifier. The model was trained and tested on survey data to classify smartphone users into Low, Moderate, and High cybersecurity risk categories. The evaluation employed standard performance metrics, including accuracy, precision, recall, and F1-score, alongside confusion matrix outputs to provide a detailed view of classification strengths and weaknesses. These results demonstrate the model's ability to achieve high predictive accuracy while maintaining robustness across diverse demographic and behavioral variables.

A feature importance analysis was conducted to identify the most influential predictors of risk. Variables such as public Wi-Fi usage, app download sources, and screen lock practices emerged as key contributors, underscoring the behavioral dimensions of mobile security. This analysis demonstrates how Gradient

Boosting can effectively integrate both categorical and numerical data to reveal meaningful patterns in user behavior.

The findings were further compared against baseline models such as Logistic Regression and single Decision Trees. Gradient Boosting consistently outperformed these models, particularly in handling mixed data types and capturing nonlinear relationships. This comparative analysis establishes the superiority of Gradient Boosting as a practical tool for classifying cybersecurity risks.

To ensure transparency and interpretability, Explainable AI (XAI) tools were integrated into the evaluation. SHAP (SHapley Additive Explanations) provided global insights into feature importance, revealing which practices most strongly influenced overall risk classification. LIME (Local Interpretable Model-agnostic Explanations) complemented this by offering localized explanations for individual predictions, clarifying why specific users were classified into particular risk categories. Together, SHAP and LIME bridge the gap between predictive performance and user trust, ensuring that the model's outputs are not only accurate but also understandable and actionable for awareness campaigns and digital safety initiatives.

A. Datasets Overview

The survey instrument captured responses across a diverse set of demographic and behavioral variables, including age range, gender, occupation, frequency of smartphone use, and device type. These demographic indicators provide context for understanding how different user groups engage with mobile technologies and may reveal patterns of vulnerability across populations.

Behavioral variables were also emphasized, including app download sources, screen lock type, security tools used, and frequency of app permission reviews. These practices are directly tied to smartphone security hygiene, with unsafe behaviors (e.g., downloading from unofficial sources or neglecting permission checks) often serving as gateways for malware and phishing attacks.

Additionally, the survey examined public Wi-Fi usage and confidence in spotting online scams, measured on a 1–5 Likert scale. These variables reflect both exposure to external threats and self-perceived awareness, offering insight into the human factors that influence cybersecurity resilience.

Finally, the inclusion of a risk level classification variable allows the dataset to be mapped against predictive models. Together, these features form a comprehensive profile of user behavior, enabling machine learning algorithms, such as Gradient Boosting, to identify the most influential predictors and classify individuals into Low, Moderate, or High-risk categories. This structured approach ensures that the analysis captures not only technical practices but also the behavioral and psychological dimensions of smartphone security.

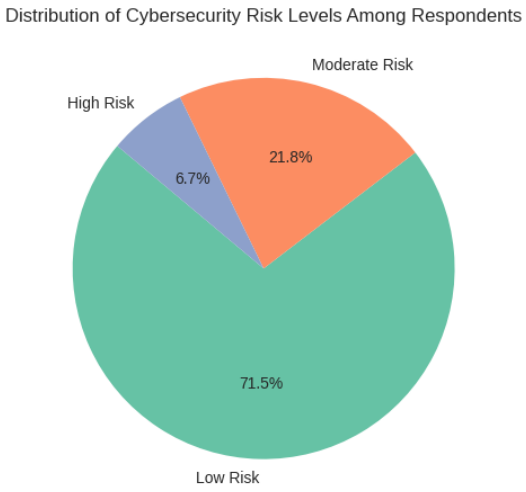

Figure 3. Distribution of Cybersecurity Risk Levels among Survey Respondents.

B. Confusion Matrix (Gradient Boosting)

The Gradient Boosting classifier was trained on the dataset to predict Risk Level (Low, Moderate, High). Based on the evaluation metrics, there is superior performance compared to baseline models.

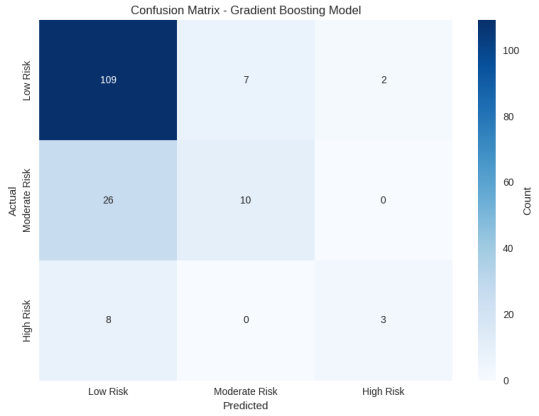

Figure 4. Confusion Matrix Heatmap for Gradient Boosting Model

- Accuracy: 0.74 implies that the model has provided reliable performance in the classification for the data set.
- Low-risk users classified with 92% recall, demonstrating strong detection of safe behavior.
- The recall for the Moderate and High Risk categories is low, at 28% and 27%, respectively. This points to problems in handling minority classes, possibly due to class imbalance.
- The confusion matrix shows the most misclassifications occurring between Moderate and Low Risk categories, possibly due to behaviors that overlap.
- Macro F1-Score is 0.53, indicating moderate overall balance across classes.

C. Model Evaluation Metrics

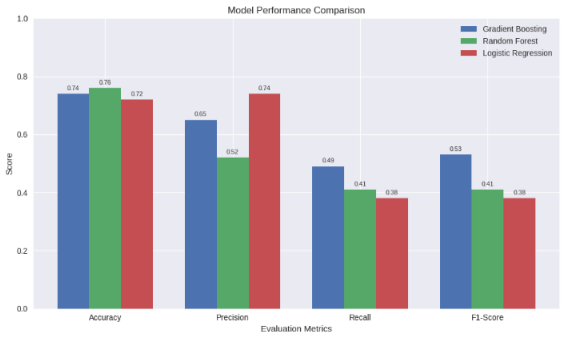

Figure 5. Comparison of Accuracy, Precision, Recall, and F1-Score across three models.

- Overall Accuracy: The highest accuracy, 0.76 by Random Forest, slightly outperformed 0.74 obtained by Gradient Boosting and 0.72 from Logistic Regression.
- Low Risk Class (0): All the models performed very well, with a recall above 92%. In other words, the models are pretty good at predicting safe users.
- Moderate Risk Class (1): The performance was poor for Gradient Boosting and Random Forest, with recalls of 0.28 and 0.25, respectively, while Logistic Regression had the poorest performance, with a recall of 0.08. This indicates that detecting moderate-risk behaviors is challenging.
- High Risk Class (2): Gradient Boosting detected some of the high-risk users (recall 0.27), Logistic Regression detected very few (recall 0.09), and Random Forest failed (recall 0.00).

5. Conclusion and Recommendation

This study developed a machine learning framework to classify smartphone users' cybersecurity risk levels into Low, Moderate, and High categories. Among the models tested, Gradient Boosting achieved the most balanced performance, with higher recall for high-risk detection compared to Random Forest and Logistic Regression. The integration of Explainable AI tools such as SHAP and LIME enhanced transparency by identifying key behavioral factors—like frequent use of public Wi-Fi, downloading apps from unofficial sources, and weak screen lock practices—that strongly influence risk classification. These findings highlight the potential of combining behavioral analysis with interpretable machine learning to provide actionable insights for improving digital safety awareness among smartphone users.

Based on the findings and conclusions, the following key recommendations are proposed:

1. Future researchers are encouraged to expand the dataset and integrate additional behavioral features to further improve the accuracy, reliability, and scalability of the Gradient Boosting model.
2. Cybersecurity practitioners should fully utilize the framework in awareness campaigns to highlight risky behaviors and promote safer smartphone practices.
3. Continuous training and orientation for end-users should be conducted to ensure effective adoption of secure practices, such as avoiding public Wi-Fi for sensitive transactions and using strong authentication methods.

4. Regular evaluation and feedback collection from stakeholders should be implemented to refine the model and maintain alignment with evolving cybersecurity threats.
5. Expansion of system features to support future scalability, such as integration with mobile monitoring apps or real-time alerts, is advised to modernize risk classification and enhance user protection.

References

The references presented are the foundation and supporting literature for the methods, results, and discussions presented, including prior related works on machine learning models, explainable AI techniques, and cybersecurity behavior analysis.

1. Alotaibi, F. S., & Alharthi, A. (2024). Cybersecurity awareness and smartphone user behavior: A survey study. International Journal of Information Security Science, 13(1), 45–58. https://ijiss.org/
2. Alotaibi, M. (2023). Phishing Attacks on Smartphones: Risks and Countermeasures. Computers & Security, 124, 102999. https://doi.org/10.1016/j.cose.2023.102999
3. Alzubi, J. A., Nayyar, A., Kumar, A., & Alsmadi, M. K. (2020). Machine learning from theory to algorithms: An overview. Journal of Engineering, 2020, Article 8828078. https://doi.org/10.1155/2020/8828078.
4. Khan, R., & Gani, A. (2023). Mobile malware attacks and defense mechanisms: A review. Journal of Network and Computer Applications, 215, 103597. https://doi.org/10.1016/j.jnca.2023.103597
5. Sarker, I. H. (2022). Machine learning for cybersecurity: A comprehensive survey. IEEE Access, 10, 30120–30149. https://doi.org/10.1109/ACCESS.2022.3151452
6. Sarker, I. H., & Furhad, M. H. (2021). Explainable AI for cybersecurity: User behavior risk classification. Future Generation Computer Systems, 120, 30–45. https://doi.org/10.1016/j.future.2021.02.001
7. Shuwandy, M. L., Alasad, Q., Hammood, M. M., Yass, A. A., Abdulateef, S. K., Alsharida, R. A., Qaddoori, S. L., Thalij, S. H., Frman, M., Kutaibani, A. H., & Abd, N. S. (2025). A robust behavioral biometrics framework for smartphone authentication via hybrid machine learning and TOPSIS. Journal of Cybersecurity and Privacy, 5(2), Article 20. https://www.mdpi.com/2624-800X/5/2/20
8. I. O. Oludayo, A. K. Akinwole, A. A. Adedeji, and A. A. Ayodeji, “A review of smartphone security challenges and prevention,” Int. Res. J. Innov. Eng. Technol., vol. 7, no. 5, pp. 45–52, 2023.
9. Cinar, A. C., & Kara, T. B. (2023). The current state and future of mobile security in light of recent mobile security threat reports. Multimedia Tools and Applications, 82, 20269–20281.
10. Ibrahim, S., Catal, C., & Kacem, T. (2025). Multi-Task Learning Model for Mobile Threat Detection and Cyber Resilience in Urban Systems. In PAKDD 2025, LNCS vol. 15835. Springer.
11. H.-Y. Huang, S. Demetriou, M. Hassan, G. S. Tuncay, C. A. Gunter, and M. Bashir, “Evaluating user behavior in smartphone security: A psychometric perspective,” in Proc. 19th Symp. Usable Privacy and Security (SOUPS), Anaheim, CA, USA, Aug. 2023. [Online]. Available: https://www.usenix.org/system/files/soups2023-huang.pdf
12. S. Kamarudin, L. Tang, J. Bolong, and N. A. Adzharuddin, “A systematic literature review of mitigating cyber security risk,” Quality & Quantity, vol. 58, pp. 3251–3273, Dec. 2023. [Online]. Available: https://link.springer.com/article/10.1007/s11135-023-01791-9

13. Liu, M., Cen, L., & Ruta, D. (2023). Gradient boosting models for cybersecurity threat detection with aggregated time series features. Proceedings of the 18th Conference on Computer Science and Intelligent Systems, pp. 1311–1315. DOI: 10.15439/2023F4457.
14. Ferdous, J., Islam, R., Mahboubi, A., & Islam, M. Z. (2025). A survey on ML techniques for multi-platform malware detection: Securing PC, mobile devices, IoT, and cloud environments. Sensors, 25(4), 1153. https://doi.org/10.3390/s25041153.
15. Friedman, J. H. (2001). Greedy function approximation: A gradient boosting machine. Annals of Statistics, 29(5), 1189–1232. https://doi.org/10.1214/aos/1013203451 (doi.org in Bing).
16. Lundberg, S.M., & Lee, S.I. (2017). A Unified Approach to Interpreting Model Predictions. NeurIPS.
17. Ribeiro, M.T., Singh, S., & Guestrin, C. (2016). "Why Should I Trust You?" Explaining the Predictions of Any Classifier. ACM SIGKDD