Predicting Cyber Attack Types Using XGBoost: A Data Mining Approach to Enhance Legal Frameworks for Cybersecurity

I Gede Agus Krisna Warmayana[1,*], Yuichiro Yamashita[2], Nobuto Oka[3]

[1]Graduate School of Humanity-Oriented Science and Engineering, Kindai University, Fukuoka, Japan

[2]National Institute of Advanced Industrial Science and Technology, Ibaraki, Japan

[3]Faculty of Humanity-Oriented Science and Engineering, Kindai University, Fukuoka, Japan

ABSTRACT

Cybersecurity threats continue to evolve rapidly, posing significant risks to organizations and challenging existing legal frameworks. This study explores the application of machine learning, specifically the XGBoost algorithm, to predict types of cyber attacks using a comprehensive dataset of cybersecurity incidents. The dataset includes organizational attributes, attack characteristics, and mitigation responses, which are preprocessed through feature scaling and encoding to support model training. Initial exploratory data analysis revealed class imbalances and variability in feature distributions, highlighting the complexity of the prediction task. The XGBoost model was trained and evaluated on an 80:20 train-test split, achieving an overall accuracy of 22.5% in multi-class classification of five common cyber attack types: Phishing, SQL Injection, DDoS, Ransomware, and Zero-Day Exploit. While the model's predictive performance was modest, feature importance analysis identified critical predictors such as geographical location, mitigation steps, and compliance standards, providing valuable interpretability. These findings underscore the potential for machine learning to support cybersecurity law enforcement by offering data-driven insights into attack patterns and organizational vulnerabilities. The ability to classify attack types can assist legal authorities and policymakers in developing targeted regulatory measures and prioritizing enforcement actions. Furthermore, the transparent nature of XGBoost's feature contributions facilitates accountability in legal contexts where automated decision-making tools are increasingly employed. However, limitations such as data imbalance and missing values affected model accuracy, suggesting the need for enhanced data collection and advanced modeling techniques in future research. Expanding datasets, incorporating real-time threat intelligence, and leveraging ensemble or hybrid algorithms may improve prediction capabilities. This study contributes to the growing intersection of data mining and cyber law by demonstrating how machine learning models can enhance legal frameworks and cybersecurity strategies. The integration of predictive analytics into cyber law enforcement holds promise for strengthening defenses against increasingly sophisticated cyber threats.

Keywords Cybersecurity, Machine Learning, XGBoost, Cyber Attack Classification, Cyber Law

Submitted 17 January 2025
Accepted 10 April 2025
Published 3 June 2025

*Corresponding author
I Gede Agus Krisna Warmayana,
2344954002e@ed.fuk.kindai.ac.jp

Additional Information and Declarations can be found on page 159

DOI: 10.63913/jcl.v1i2.8

Introduction

In the digital age, the significance of cybersecurity has escalated dramatically due to the increasing reliance on internet-based technologies for both personal and professional endeavors. Cybersecurity encompasses a wide range of practices and technologies designed to safeguard sensitive information from

unauthorized access, attacks, and damage. The rise of cyber threats, including data breaches, ransomware, and identity theft, has made cybersecurity a paramount concern for organizations and individuals alike. According to Bhange [1], a robust understanding of cyber law is crucial as it sets the legal framework for regulating online activities and protecting digital assets, thereby ensuring accountability and compliance with various laws. This legal context is essential as cybersecurity alone cannot sufficiently protect against the evolving and sophisticated nature of cyber threats.

As organizations continue to expand their digital footprints, the integration of cybersecurity measures is becoming integral to operational effectiveness. Smajić [2] emphasizes that companies must leverage key cybersecurity pillars to build a resilient workforce and protect sensitive data. Furthermore, advances in cybersecurity frameworks and information security standards offer structured methodologies that organizations can apply to comply with legal mandates and enhance their cyber defense strategies. Taherdoost [3] discusses how established cybersecurity standards help organizations create compliance protocols that address cyber threats and facilitate accountability. By adhering to these frameworks, businesses can not only protect their assets but also uphold customer trust, which is vital in maintaining a competitive advantage in today's market [4], [5].

The dynamic nature of cyber threats necessitates continuous evolution of both security measures and legal frameworks. In this context, international cyber law has become increasingly critical. As highlighted by Farabi et al. [6], countries are developing and updating cyber laws to mitigate risks associated with growing cyber threats. These laws facilitate international cooperation and establish norms that govern cyber conduct across borders, crucial for addressing transnational cybercrime effectively. Moreover, Kour and Pierce [7] emphasize the persistent challenges organizations face in implementing cybersecurity policies, particularly in an ever-changing threat landscape that demands constant vigilance and adaptation.

The rise of cyber attacks has become a pressing challenge for organizations globally, evolving in sophistication and variety due to the rapid digitalization of services and infrastructure. Cyber attacks are broadly classified into several types, including phishing, ransomware, denial-of-service (DoS) attacks, and advanced persistent threats (APTs), among others. Each attack type poses distinct risks and can result in severe consequences for organizations, ranging from financial loss to reputational damage. Phishing, often considered one of the most prevalent forms of cyber attack, involves fraudulent attempts to obtain sensitive information by masquerading as a trusted entity. Nayak et al [8] highlight that phishing can lead to unauthorized access to sensitive data and significant financial losses. In 2021 alone, phishing attacks accounted for over 30% of all data breaches, emphasizing the necessity for organizations to prioritize cybersecurity measures. Similarly, ransomware attacks, where malicious software encrypts an organization's data and demands a ransom for decryption, have surged dramatically in recent years. Bilen and Özer [9] document that ransomware attacks can incapacitate entire infrastructures, leading to substantial operational disruptions and financial repercussions. For instance, the Colonial Pipeline attack in May 2021 resulted in fuel shortages across the Eastern United States, showcasing the extensive impact these attacks can have on critical infrastructure.

DoS attacks, which seek to render a service unavailable by overwhelming it with traffic, can significantly affect an organization's ability to operate, thus impacting revenue and customer trust. The consequences of such attacks can lead to lost sales and diminished customer loyalty, producing a ripple effect across the economy. Perusquía [10] discusses how the increasing sophistication of DoS attacks complicates detection and mitigation efforts. Additionally, APTs are sophisticated, multi-stage attacks typically targeting high-value information over long periods, often involving state-sponsored actors. These attacks are particularly concerning due to their covert nature and potential to extract sensitive intellectual property, or engage in espionage [11].

The need for predictive models in cybersecurity is becoming increasingly significant as organizations confront an escalating volume and complexity of cyber threats. These models not only enhance the efficacy of cybersecurity strategies but also contribute to the development of more robust legal frameworks. Predictive analytics can play a crucial role in anticipating and mitigating potential cyber threats before they manifest into serious incidents. Predictive models play a crucial role in strengthening cybersecurity by enabling early detection and classification of cyber threats. By accurately predicting the types of cyber attacks, these models provide valuable insights that help organizations anticipate potential risks and respond proactively. This capability not only enhances technical defenses but also supports legal frameworks by offering evidence-based information that can guide law enforcement and policymakers in drafting more effective cyber laws and regulations. In this way, predictive analytics bridges the gap between technological defense and legal accountability, making cybersecurity efforts more comprehensive and robust.

The main objective of this study is to develop a predictive model using data mining techniques, specifically the XGBoost algorithm, to classify various types of cyber attacks accurately. By leveraging a dataset of cyber incidents, the model aims to assist legal authorities and cybersecurity professionals in identifying attack patterns, thereby facilitating timely legal actions and prevention strategies. This research seeks to demonstrate how machine learning can contribute not only to improving organizational security but also to supporting the enforcement of cyber laws by providing actionable intelligence for combating cybercrime.

Literature Review

Data Mining in Cybersecurity

Data mining techniques have emerged as a crucial element in enhancing cybersecurity measures, facilitating the development of robust prediction models that can help mitigate and respond to various cyber threats. Algorithms such as Support Vector Machines (SVM), Random Forest, and XGBoost are frequently employed in studies to identify and predict cyber threats effectively. SVM are popular for their ability to classify high-dimensional data effectively. In a study by Jimoh and Al-Juboori [12], SVM was utilized to secure medical devices, specifically pacemakers, demonstrating its capability in monitoring network traffic to preempt unauthorized access and attacks. The study highlights how SVM can predict security breaches by processing intricate features derived from network usage patterns. Similarly, Chowdhury et al [13] confirm that SVM, along with other techniques, enhances early threat detection by analyzing historical data to identify potential patterns—thus enabling organizations to

implement proactive measures. Such capabilities position SVM as a vital tool in the broader ecosystem of cybersecurity solutions.

Random Forest is another powerful algorithm frequently applied in cybersecurity. Rishad's [14] comparative analysis emphasizes its effectiveness alongside other machine learning models in detecting various cybersecurity threats, from ransomware to insider threats. The study demonstrates that Random Forest outperforms traditional methods by achieving high levels of accuracy, thereby enhancing an organization's ability to respond effectively to potential threats. Moreover, Nwafor et al [15] argue that Random Forest's ensemble approach enables a refined analysis of financial datasets, leading to improved performance in forensic investigations within financial markets, which is vital for maintaining security in sensitive sectors. XGBoost, known for its efficiency and performance, has also been increasingly adopted in cybersecurity applications. In Rishad's study [14], XGBoost is highlighted as one of the models that yield superior performance metrics, including high AUC-ROC scores, confirming its efficacy in real-time threat detection. The algorithm's iterative approach allows for improved generalization on complex datasets, making it particularly valuable in environments with high-dimensional features, such as those encountered in network security operations.

Data mining's application in cybersecurity extends beyond these algorithms and encompasses advanced techniques aimed at enhancing predictive capabilities. Gulati et al. discuss the scope of artificial intelligence components, including data mining, highlighting their role in transforming cybersecurity practices. This paper underscores the urgency of employing advanced analytics to combat emerging threats as traditional security systems struggle to keep pace with rapid technological advancements [16]. Furthermore, the integration of user behavioral data for predictive analytics, as explored by Addae et al [17], reveals how such information can be harnessed to create adaptive cybersecurity measures. This adaptability is crucial to countering the increasingly sophisticated nature of cyber attacks. By employing data mining techniques, organizations can build user profiles that enable tailored security responses, mitigating risks associated with unique user behaviors.

Relevance of Predictive Models in Legal Context

Predictive models have gained momentum in the context of mitigating cybercrime, and their integration enhances existing legal frameworks by providing actionable insights that facilitate proactive measures against cyber threats. By utilizing advanced data analytics, these models can significantly improve the understanding of cyber threats and enhance the capacity of legal frameworks to respond effectively. In the specific domain of fintech, Odio et al [18] present a cybersecurity maturity model that incorporates predictive analytics to transition firms from basic to advanced security measures. This structured approach enables organizations to recognize vulnerabilities based on historical attack data and internal security metrics, allowing legal frameworks to adapt and enforce regulations that reflect the evolving complexity of cyber threats. Consequently, this model strengthens cybersecurity practices and reinforces the legal obligations firms hold to protect client data and integrity.

Kumar and Sinha [19] further emphasize the importance of pattern analysis of cybercrime incidents in building predictive models that support law enforcement agencies. By identifying attack vectors and behavioral patterns, predictive

analytics can guide the development of legal policies aimed at specific cyber threats. Such data-driven insights allow legislators to construct targeted laws that address prevalent risks, ultimately improving the legal landscape governing cybersecurity. Incorporating machine learning into predictive models strengthens their effectiveness in combating cyber threats. Singh et al [20] explain that intelligent systems facilitate the early detection of vulnerabilities and support compliance with legal standards by identifying breaches before they escalate into legal liabilities. By continuously learning from new data, these systems contribute to refining legal regulations applicable to cybersecurity, ensuring they remain relevant amidst rapid technological advancements.

Cyber Attack Classification

The increasing prevalence of cyber attacks necessitates effective classification models in cybersecurity to enhance detection, response, and mitigation strategies. Among these, XGBoost has emerged as a powerful algorithm for predicting attack types due to its high performance and flexibility. This discussion focuses on the advantages and challenges associated with applying XGBoost within the context of cyber attack classification. One of the critical advantages of using XGBoost in cybersecurity is its ability to handle large and complex datasets efficiently. Sharma's [21] comparative analysis highlights that XGBoost achieved an impressive accuracy rate of 98% compared to other machine learning models in detecting cyber threats, including sophisticated attack patterns. This capability arises from its underlying gradient boosting framework, which optimizes prediction accuracy by combining weak learner predictions. As a result, XGBoost is adept at identifying various attack types, including those characterized by subtle and complex behaviors, thereby significantly improving intrusion detection systems (IDS).

Moreover, XGBoost exhibits excellent performance in dealing with imbalanced datasets, common in cyber attack classification tasks. Utilizing techniques such as SMOTE allows the model to maintain high accuracy while classifying underrepresented attack types. However, Airlangga's study [22] indicates that while XGBoost did show improved classification capabilities in detecting denial-of-service (DDoS) attacks, it did not outperform Random Forest in terms of classification accuracy. This flexibility in preprocessing supports the model's effectiveness across different attack categories, enhancing its applicability in various cybersecurity contexts. Despite its advantages, the application of XGBoost in cybersecurity is not without challenges. Notably, the complexity of model tuning can pose difficulties for practitioners, particularly those with limited quantitative expertise. The hyperparameter optimization process is critical for maximizing the performance of XGBoost models, necessitating a nuanced understanding of how adjustments impact outcomes. Additionally, the iterative nature of gradient boosting may lead to overfitting, especially in scenarios with limited training data or excessive noise. Goyal et al [23] discuss the importance of employing appropriate regularization techniques to ensure that models remain generalizable across different unseen attack vectors.

Method

Figure 1 outlines our end-to-end methodology, which starts with data loading and exploratory analysis, progresses through preprocessing and the development of an XGBoost model, and concludes with model evaluation and feature importance analysis.

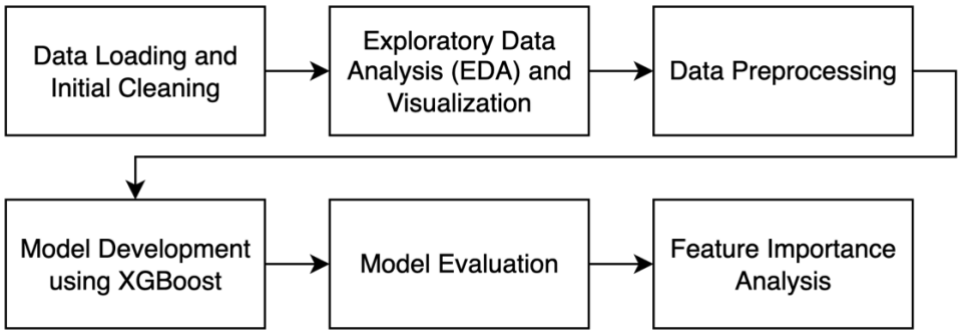

Figure 1 Research Method Flowchart

Data Loading and Initial Cleaning

The dataset used in this study was loaded from a CSV file containing detailed records of cybersecurity incidents, including business-related features, attack characteristics, and response measures. Initially, irrelevant columns such as Attack_ID and Timestamp were removed to focus the analysis on meaningful attributes that contribute to predicting the attack type. Boolean features present in the dataset were converted into integer format (0 or 1) to ensure compatibility with machine learning algorithms. The dataset was then examined for missing values; in this case, no significant missing data was found, so no imputation was necessary. This initial cleaning step was crucial to prepare the dataset for reliable analysis and modeling.

Exploratory Data Analysis (EDA) and Visualization

Exploratory Data Analysis was conducted to gain insights into the structure and distribution of the data. The distribution of the target variable, Attack_Type, was visualized using count plots, which revealed the frequency of each attack class and helped assess class imbalance issues. Numerical features were statistically summarized and visualized with histograms and kernel density estimates to understand their distributions and detect any anomalies. Correlation heatmaps of numerical variables were also generated to identify relationships between features, which could inform feature selection or engineering. Categorical features were analyzed for their cardinality, and those with very high unique value counts were dropped to reduce dimensionality and potential noise, ensuring a more effective model training process.

Data Preprocessing

To prepare the data for machine learning, the features were divided into numerical and categorical types. Numerical features were standardized using the StandardScaler method to normalize their scales, which is essential for algorithms sensitive to feature magnitudes. Categorical variables were transformed using one-hot encoding to convert them into binary vectors, enabling the model to process non-numeric data effectively. The target variable, Attack_Type, was encoded into numeric labels using LabelEncoder to facilitate multi-class classification. The preprocessed dataset was then split into training and testing subsets in an 80:20 ratio, with stratified sampling employed to preserve the original class distribution in both sets, which is vital for unbiased model evaluation.

Model Development Using XGBoost

The classification model chosen for this research was XGBoost, a gradient boosting framework known for its efficiency and high performance on tabular data. The model was configured with a multi-class softmax objective, suitable for predicting multiple attack categories. An integrated pipeline was constructed to sequentially perform preprocessing and model training, which ensured that transformations were consistently applied during both training and prediction phases. The XGBoost classifier was trained on the training data, and the training duration was recorded to assess computational efficiency. Hyperparameters such as the number of classes and evaluation metric (mlogloss) were explicitly defined, while other parameters were left at their defaults but can be fine-tuned in future work.

Model Evaluation

After training, the model's performance was evaluated on the test set using multiple metrics. Overall accuracy was calculated to measure the proportion of correctly classified instances. Precision, recall, and F1-score were reported per class to provide a detailed understanding of the model's predictive quality, especially important in imbalanced multi-class scenarios. A confusion matrix was generated and visualized to identify specific classes where the model performed well or struggled, enabling targeted improvements. These evaluation steps ensured a comprehensive assessment of the classifier's effectiveness in correctly predicting cyber attack types.

Feature Importance Analysis

To interpret the model's decision-making process, feature importance scores were extracted from the trained XGBoost model. These scores quantify the contribution of each feature in the classification task, offering insights into which variables most influence the prediction of attack types. Both numerical and one-hot encoded categorical features were combined for this analysis. The top 20 most important features were presented in a ranked table and visualized using a bar plot, facilitating intuitive understanding. This interpretability aspect is crucial for cybersecurity stakeholders and legal professionals who require transparency in predictive models to justify decisions and policies based on model outputs.

Result and Discussion

Data Loading and Initial Exploration

The dataset, consisting of 1,000 cybersecurity incident records and 26 attributes, was successfully loaded and initially inspected to ensure data quality. After removing irrelevant identifiers (Attack_ID and Timestamp), the dataset was reduced to 24 features relevant for analysis. A thorough check for missing values revealed that some columns, such as Malware_Name, Exploit_Method, Data_Compromised, and Compliance_Standards, contained substantial missing data—331, 167, 187, and 339 missing entries respectively. Despite this, critical columns including the target variable Attack_Type and many key features remained complete, allowing for robust modeling without requiring extensive imputation. Boolean columns such as Legal_Action_Taken, Employee_Training, Use_of_MFA, and Data_Backup_Availability were converted into binary integers (0 or 1) to facilitate their inclusion in the machine learning pipeline. The dataset contained a mix of categorical and numerical data types, requiring careful preprocessing.

Exploratory Data Analysis (EDA)

The analysis of the target variable revealed five distinct categories of cyber attacks: Phishing, SQL Injection, DDoS, Ransomware, and Zero-Day Exploit. Phishing was the most prevalent attack type with 296 instances, making it the dominant category in the dataset, followed by SQL Injection with 210 cases and DDoS attacks with 183 cases. The other categories, Ransomware and Zero-Day Exploits, had fewer instances, 180 and 131 respectively. This distribution indicated a class imbalance, which has implications for model training and evaluation. The cardinality check on categorical variables identified Payload_Details as having 50 unique values—considerably higher than the threshold set for manageable cardinality—so this feature was dropped to reduce the dimensionality and complexity of the model. The remaining categorical features had between 2 and 20 unique values, making them suitable for encoding.

Statistical summaries of numerical features revealed a wide range in values. For example, Financial_Loss averaged around 28,940 units with a high standard deviation, reflecting diverse financial impacts across incidents. Incident_Response_Time ranged broadly, with some organizations responding very quickly while others took significantly longer, averaging 106 minutes. Other impact-related features such as Operational_Disruption and Reputation_Damage_Score further highlighted variability in incident severity and organizational consequences. Visualizations such as histograms for numerical variables and count plots for categorical features were generated to explore these distributions and assist in identifying potential outliers or skewed data. A correlation heatmap showed weak to moderate relationships between some numerical features, which could influence model performance.

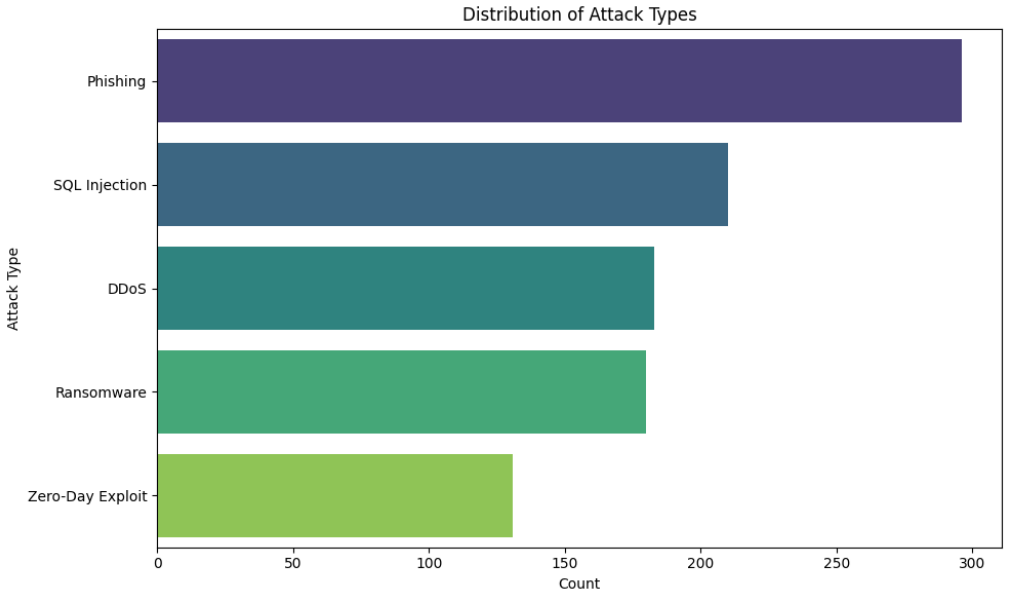

Figure 2 Distribution of Attack Types

Figure 2 shows the distribution of cyber attack types within the dataset. Phishing emerges as the most frequent attack type, significantly more common than others, followed by SQL Injection, DDoS, Ransomware, and Zero-Day Exploit. This distribution highlights the relative prevalence of different attack methods,

indicating that phishing remains a major threat in cybersecurity incidents.

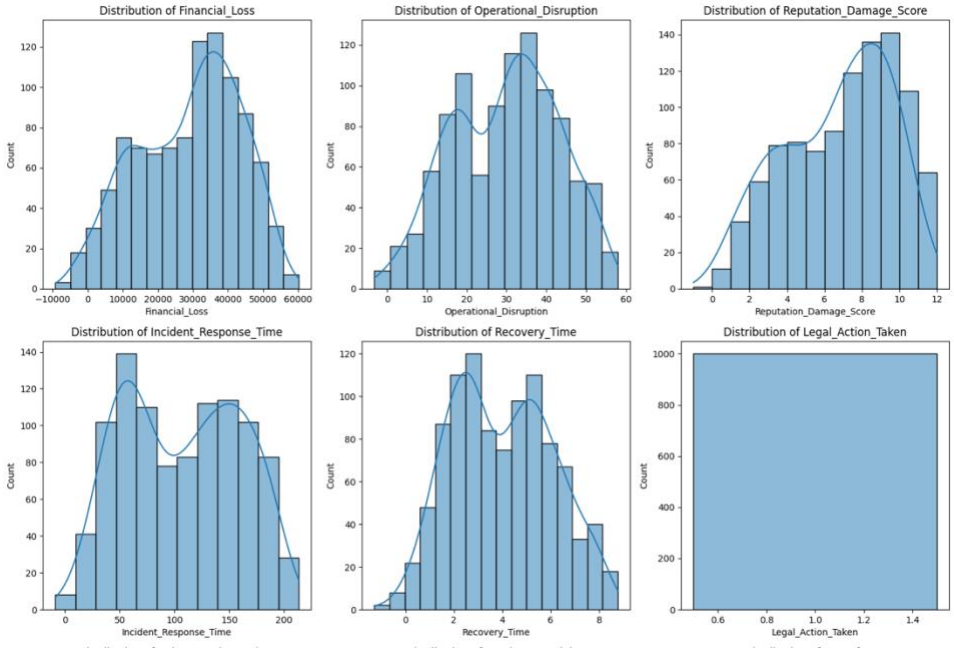

Figure 3 Histogram of Numerical Features

Figure 3 presents a series of histograms with kernel density estimates illustrating the distributions of various numerical features. Financial Loss shows a right-skewed distribution with many incidents incurring moderate to high losses, although some cases involve negative or minimal losses. Operational Disruption also varies widely across incidents, indicating the diverse impact on business continuity. The Reputation Damage Score centers around mid to high values, suggesting that many attacks cause notable reputational harm. Incident Response Time and Recovery Time both display multi-modal distributions, reflecting differences in how quickly organizations detect and recover from attacks. The Legal Action Taken, Employee Training, Use of MFA, and Data Backup Availability features are binary and appear as single bars, indicating full or nearly full compliance within the dataset. The Cybersecurity Budget has a wide spread, with some organizations investing heavily while others allocate minimal resources.

Data Splitting and Model Training

The cleaned dataset was split into training and testing subsets with an 80:20 ratio, using stratified sampling to preserve the distribution of attack types across both sets. This approach ensures the model is trained and evaluated on representative samples from all classes. The multi-class target variable Attack_Type was encoded into numerical labels using LabelEncoder, mapping classes as follows: DDoS (0), Phishing (1), Ransomware (2), SQL Injection (3), and Zero-Day Exploit (4).

A machine learning pipeline was constructed integrating data preprocessing steps—standard scaling for numerical features and one-hot encoding for categorical features—with an XGBoost classifier configured for multi-class softmax classification. Model training was efficient, completing in approximately 15 seconds, demonstrating the practicality of the approach for cybersecurity

datasets of this size.

Model Evaluation and Performance

The trained XGBoost model achieved an overall accuracy of 22.5% on the test set, indicating a relatively modest predictive capability given the multi-class nature and complexity of the problem. The classification report detailed class-specific performance metrics: DDoS attacks had the highest precision (31%) and recall (30%), suggesting the model was better at correctly identifying this category. Phishing attacks had moderate recall (31%) but lower precision (21%), implying some misclassification. Ransomware and Zero-Day Exploit categories were predicted with notably lower precision and recall, especially the latter, with a recall of only 4%, indicating frequent misclassification and model difficulty in recognizing these rarer or more complex attack types.

The confusion matrix (figure 4) visualized these prediction patterns, highlighting where the model frequently confused certain classes. For instance, the model often misclassified Phishing and SQL Injection attacks, which might share overlapping features or similar organizational contexts. Zero-Day Exploits, due to their rarity and subtle characteristics, were the most commonly misclassified attacks, sometimes confused with other categories or overlooked entirely. These results underscore the challenges in multi-class cybersecurity attack prediction, where some classes are inherently harder to distinguish based on available data.

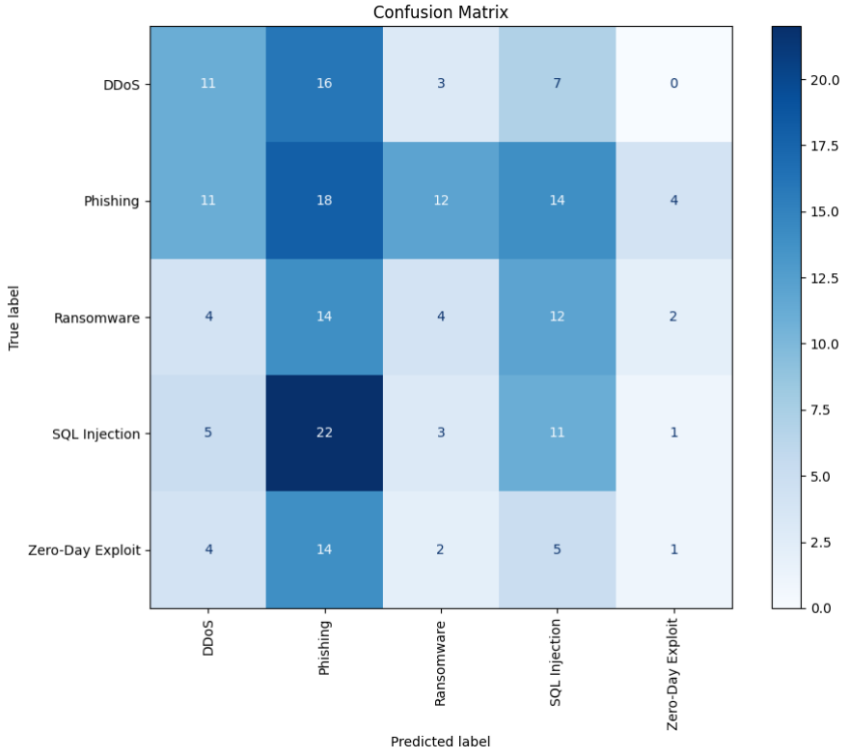

Figure 4 Confusion Matrix

Feature Importance and Interpretability

The model's feature importance analysis (figure 5) provided valuable insights into which variables most strongly influenced classification decisions. Geographical features, such as Geographical_Location_Brazil and

Geographical_Location_UK, emerged as top predictors, suggesting that attack types vary significantly by region or that detection/reporting patterns differ geographically. Several mitigation-related features (e.g., Mitigation_Steps_Mitigation 4, Mitigation_Steps_Mitigation 14) ranked highly, reflecting that specific response strategies may correlate with particular attack categories. Business sector features like Business_Type_Manufacturing and compliance standards such as Compliance_Standards_NIST also contributed notably, indicating organizational context impacts vulnerability or attack profile. Exploit methods such as Exploit_Method_Social Engineering played a significant role, consistent with the known importance of social engineering in cyber threats. Detection methods and affected systems (e.g., Detection_Method_User Report, Affected_Systems_ERP) were among other influential features, reinforcing the relevance of monitoring and system type in predicting attack categories. This feature-level interpretability is critical for cybersecurity practitioners and policymakers, enabling more targeted defenses and legal frameworks tailored to prevalent attack characteristics.

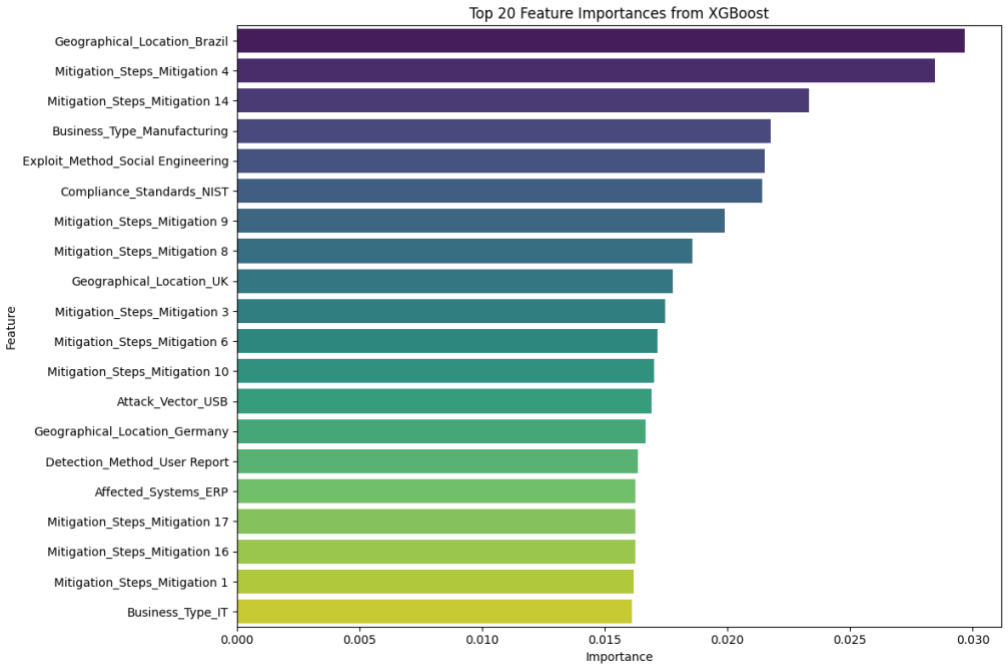

Figure 5 Feature Importance Analysis

Discussion

Compared to other machine learning models such as SVM and Logistic Regression, XGBoost generally offers enhanced prediction accuracy due to its ability to capture complex nonlinear relationships and interactions between features. While SVM and Logistic Regression are effective for certain classification tasks, especially with smaller or linearly separable datasets, XGBoost's ensemble-based boosting technique often yields better performance on large, structured datasets like those in cybersecurity. However, in this study, the overall accuracy of XGBoost was modest, indicating that even advanced models face challenges in accurately classifying diverse cyber attack types. Despite this, XGBoost's superior ability to highlight feature importance provides valuable interpretability advantages over simpler models, making it a more relevant choice for applications that require explainability, such as cyber law

enforcement.

The findings from this predictive modeling study have meaningful implications for cybersecurity law and policy development. By identifying key features that influence attack classification—such as geographical location, mitigation steps, and compliance standards—lawmakers and regulators can better understand the evolving threat landscape and tailor legal frameworks accordingly. The ability to predict attack types, even with limited accuracy, supports proactive risk assessment and prioritization of regulatory efforts in vulnerable sectors or regions. Moreover, transparent models like XGBoost facilitate accountability and trust in automated decision systems, which is critical when these tools are used to support legal investigations and enforcement actions. Ultimately, integrating predictive analytics into cybersecurity policy can help bridge the gap between technical defense mechanisms and legal protections, fostering a more resilient digital ecosystem.

Conclusion

This research demonstrated that machine learning, specifically the XGBoost algorithm, can be applied to classify various types of cyber attacks based on organizational and attack-related features. Although the overall prediction accuracy was moderate, the model effectively identified important features such as geographical location, mitigation steps, and compliance standards that influence attack classification. These findings highlight the potential of predictive analytics to support cybersecurity efforts by providing actionable insights into attack patterns and characteristics. From a practical standpoint, the study's results can be valuable for legal and regulatory bodies in enhancing cybersecurity frameworks. By understanding which factors are most indicative of specific cyber threats, policymakers can develop more targeted laws and guidelines to prevent and respond to cyber attacks. Additionally, the ability to predict attack types contributes to more efficient resource allocation for investigation and enforcement, strengthening the legal response to cybercrime. Transparent and interpretable models like XGBoost also foster trust and accountability when machine learning tools are integrated into cyber law enforcement practices. Despite these promising outcomes, the study faced several limitations, including the moderate predictive accuracy and challenges arising from imbalanced class distribution and missing data in some features. Future research should explore advanced data augmentation techniques, incorporation of additional contextual data, and ensemble modeling approaches to improve classification performance. Moreover, expanding the dataset to include more diverse cyber attack instances and continuously updating models with emerging threats will enhance their relevance. Ultimately, ongoing efforts to refine machine learning applications in cybersecurity law enforcement are essential to keep pace with the rapidly evolving digital threat landscape.

Declarations

Author Contributions

Conceptualization: I.G.A.K.W.; Methodology: Y.Y.; Software: N.O.; Validation: Y.Y.; Formal Analysis: I.G.A.K.W.; Investigation: N.O.; Resources: Y.Y.; Data Curation: N.O.; Writing Original Draft Preparation: I.G.A.K.W.; Writing Review and Editing: N.O.; Visualization: I.G.A.K.W.; All authors have read and agreed to the published version of the manuscript.

Data Availability Statement

The data presented in this study are available on request from the corresponding author.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Mr. B. M. Bhange, "Understanding Cyber Law and Security," *Gimrj*, vol. 13, no. 3, pp. 41-44, 2025, doi: 10.69758/gimrj/2503i3iivxiiip0007.

[2] N. SMAJIĆ, "Human Element in Cybersecurity. Strategies for Building a Stronger and More Secure Workforce," *Int. J. Inf. Secur. Cybercrime*, vol. 12, no. 1, pp. 30-36, 2023, doi: 10.19107/ijisc.2023.01.04.

[3] H. Taherdoost, "Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview," *Electronics*, vol. 11, no. 14, p. 2181, 2022, doi: 10.3390/electronics11142181.

[4] W. A. Khan, "Collaborating With C-Level Executives to Align Security With Business Goals: How Strategic Security Initiatives Were Integrated With Broader Business Objectives," *J. Eng. Appl. Sci. Technol.*, vol. 2024, no. 6, pp. 1-11, 2024, doi: 10.47363/jeast/2024(6)e137.

[5] A. M. Wahid, T. Hariguna, and G. Karyono, "Optimization of Recommender Systems for Image-Based Website Themes Using Transfer Learning," *J. Appl. Data Sci.*, vol. 6, no. 2, pp. 936-951, Mar. 2025, doi: 10.47738/jads.v6i2.671.

[6] S. F. Farabi, A. P. Dr. H. K. Abdul Al, Md. O. Faruque, and S. Akter, "The Impact of the US on the Development of International Cybersecurity Law: Legal Challenges and Emerging Norms," *Ilprom*, vol. 2024, no. 8, pp. 1-10, 2024, doi: 10.63471/hi240004.

[7] M. Kour and J. Pierce, "Cybersecurity Policies Implementation," vol. 2024, no. 5, pp. 149-179, 2024, doi: 10.4018/979-8-3693-0839-4.ch007.

[8] M. P. Nayak, M. Sufiyan, N. S. Monisha, M. G. Bhaskar, and M. Raju, "Review Paper on Cyber Security and Types of Cyber Attacks," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 2022, no. 6, pp. 732-735, 2022, doi: 10.48175/ijarsct-7043.

[9] A. Bilen and A. B. Özer, "Cyber-Attack Method and Perpetrator Prediction Using Machine Learning Algorithms," *Peerj Comput. Sci.*, vol. 7, no. 3, p. e475, 2021, doi: 10.7717/peerj-cs.475.

[10] J. A. Perusquía, "Bayesian Models Applied to Cyber Security Anomaly Detection Problems," *International Statistical Review,* vol. 90, no. 1, pp. 78-99, 2020, doi: 10.1111/insr.12466.

[11] M. R. Al-Mousa, "Analyzing Cyber-Attack Intention for Digital Forensics Using Case-Based Reasoning," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 6, pp. 3243-3248, 2019, doi: 10.30534/ijatcse/2019/92862019.

[12] S. T. Jimoh and S. Al-Juboori, “Cyber-Securing Medical Devices Using Machine Learning: A Case Study of Pacemaker,” *J. Inform. Web Eng.*, vol. 3, no. 3, pp. 271-289, 2024, doi: 10.33093/jiwe.2024.3.3.17.
[13] R. H. Chowdhury, N. U. Prince, S. M. Abdullah, and L. A. Mim, “The Role of Predictive Analytics in Cybersecurity: Detecting and Preventing Threats,” *World J. Adv. Res. Rev.*, vol. 23, no. 2, pp. 1615-1623, 2024, doi: 10.30574/wjarr.2024.23.2.2494.
[14] S. M. Shadul Rishad, “Leveraging Ai and Machine Learning for Predicting, Detecting, and Mitigating Cybersecurity Threats: A Comparative Study of Advanced Models,” *Ijcsis*, vol. 10, no. 1, pp. 1-10, 2025, doi: 10.55640/ijcsis/volume10issue01-02.
[15] K. C. Nwafor, D. O. T. Ihenacho, and P. W. Nyanda, “Leveraging Data Mining and Cybersecurity Techniques to Enhance Algorithmic Trading Performance and Forensic Investigations in Financial Markets,” *Int. J. Sci. Res. Arch.*, vol. 13, no. 1, pp. 3091-3106, 2024, doi: 10.30574/ijsra.2024.13.1.2039.
[16] P. Gulati, U. Gulati, H. Uygun, and R. Gujrati, “Artificial Intelligence in Cyber Security: Rescue or Challenge,” *Rev Artif Intell Educ*, vol. 4, no. 1, p. e07, 2023, doi: 10.37497/rev.artif.intell.education.v4i00.7.
[17] J. Addae, X. Sun, D. Towey, and M. Radenkovic, “Exploring User Behavioral Data for Adaptive Cybersecurity,” *User Model. User-Adapt. Interact.*, vol. 29, no. 3, pp. 701-750, 2019, doi: 10.1007/s11257-019-09236-5.
[18] P. E. ODIO, R. Okon, M. O. Adeyanju, E. Kokogho, and O. C. Onwuzulike, “Developing a Cybersecurity Maturity Model for Fintech Firms Using Predictive Analytics,” *Int. J. Sci. Technol. Res. Arch.*, vol. 8, no. 1, pp. 23-49, 2025, doi: 10.53771/ijstra.2025.8.1.0021.
[19] S. Kumar and P. K. Sinha, “Pattern Analysis of Cyber Crime Incidents to Predict Occurrence and Selection of the Best Technology to Prevent IT,” *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 10, no. 6, pp. 624-629, 2024, doi: 10.32628/cseit241061104.
[20] B. Singh, C. Kaunert, and S. Chandra, “Relishing Machine Learning Intelligence Combating Cyber Threats,” vol. 2025, no. 2, pp. 1-45, 2025, doi: 10.4018/979-8-3693-6250-1.ch007.
[21] V. Sharma, “Comparative Analysis of Machine Learning Models for Intrusion Detection Systems,” *PMJ*, vol. 35, no. 3, pp. 273-285, 2025, doi: 10.52783/pmj.v35.i3s.3891.
[22] G. Airlangga, “Detection of DDoS Attacks in UAV Communication Networks Using Machine Learning Models,” *Jurasik J. Ris. Sist. Inf. Dan Tek. Inform.*, vol. 10, no. 1, p. 403, 2025, doi: 10.30645/jurasik.v10i1.882.
[23] D. Goyal, F. Sheth, P. Mathur, and A. K. Gupta, “Discrete Mathematical Models for Enhancing Cybersecurity : A Mathematical and Statistical Analysis of Machine Learning Approaches in Phishing Attack Detection,” *J. Discrete Math. Sci. Cryptogr.*, vol. 7, no. 2, pp. 569-599, 2024, doi: 10.47974/jdmsc-1893.