ENHANCING CYBER THREAT DETECTION IN INDIA USING SUPERVISED MACHINE LEARNING TECHNIQUES

A. Jeya Shanthi
Assistant Professor, Department of BCA, K.M.G College of Arts and Science Gudiyatham & Research Scholar of Dr.M.G.R. University, Chennai, Tamil Nadu

K. Latha
Assistant Professor & Research Scholar, School of Computer Science Takshashila State Private University, Ongur, Tindivanam, Tamil Nadu
https://doi.org/10.34293/9789361639715.shanlax.ch.010

Abstract

India's swift digital growth has created extraordinary prospects while also presenting major cybersecurity hurdles. This research makes use of the Indian Cybersecurity Threats Dataset (2015–2024) to examine and categorize different cyberattacks impacting crucial sectors such as finance, healthcare, and governance. Two supervised machine learning models, k-Nearest Neighbors (k-NN) and Random Forest, were employed to sort cyber incidents according to threat category, method of attack, and level of impact. The process of data preparation involved techniques such as label encoding, feature scaling, and dividing the data into training and testing sets. Assessment of the models through metrics like precision, recall, F1-score, and accuracy revealed that Random Forest surpassed k-NN, achieving flawless classification accuracy. These findings highlight the capability of ensemble learning methods to improve the detection and response to cyber threats. The research supports ongoing incorporation of advanced AI techniques within India's cybersecurity strategy to effectively tackle emerging digital threats.

Keywords: *Indian Cybersecurity, Machine Learning, Random Forest, k-Nearest Neighbors, Cyber Threat Classification, Digital Security*

Introduction

India, as a country that has gone through a rapid improvement in its digital infrastructure, and an increase in internet use, has been transforming significantly in the recent past. Almost every sector such as finance, health, education, and e-government have embraced the use of digital technology in their operations. However, this progress has predisposed the country to other cyber threats such as phishing, malware, data theft, and ransomware. Cybersecurity concerns on a national level have become even more urgent as the number of digital transactions and cloud services usage exposes essential information systems to cyber threats.

The Government of India has responded to these increasing threats by implementing various initiatives such as the National Cyber Security Policy, formation of Indian Computer Emergency Response Team (CERT-In), and the Digital India project. These measures aim to contribute to a secure cyber ecosystem through the growth of awareness by increasing technical competence and legal frameworks. Nevertheless, even these attempts do not prevent the increasing sophistication of cyberattacks, which requires the continuous development of defence solutions and the active identification of threats, as well as the integration of the latest information technologies into cybersecurity operations, including artificial intelligence and machine learning.

Review of Literature

Cybersecurity in India has undergone significant change over the past decade driven by the rapid process of cyber digitalization in the country. Tripathy (2025) presents a comprehensive analysis of trends in cybercrime evolution over time because the category of risks such as ransomware, data leaks, and social manipulation have become more sophisticated. The review of the literature by Verma and Shri (2022) demonstrated an influx of scholarly and institutional attention to cybersecurity, especially in such fields as finance, healthcare, and education. Yadav (2021) also explores the growing risk of phishing attacks, highlighting the need to focus on raising awareness and implement more strict regulations to make user-level vulnerabilities fewer.

Considering such emerging threats, researchers have gradually started to leverage machine learning and artificial intelligence as assets in safeguarding against cyber-attacks. Chowdhury et al. (2024) and Gangavarapu et al. (2020) analyze how adaptive artificial intelligence systems and, in particular, systems based on supervised learning are used to fight phishing and malware threats. Neural network models such as that shown by Martin et al. (2011) and ensemble approaches such as the Random Forests model by Rathore et al. (2019) and the Sharma et al. (2019) have demonstrated high effectiveness in recognizing advanced attacks. Gupta et al. (2019) confirm these findings, showing that combined strategies are more effective than single classifiers in the systems that are built to detect intrusion. The combination of these studies demonstrates that more and more researchers rely on predictive analytics to reinforce the cybersecurity system in India.

On the policy and governance level, the Indian government has also introduced some major initiatives that could help to create a robust cyber environment. The development of CERT-In and the introduction of the National Cyber Security Policy are two of the main success stories aimed at improving how threats are dealt with and the promotion of safe online behavioural practices.. Nevertheless, Adholiya and Adholiya (2019) note that there is a consistent knowledge gap among users, especially semi-urban and rural areas. Moreover, issues of the ethical aspects of cybersecurity have also been mentioned, as it was observed in the instance of the alleged abuse of the hacking services by Appin. Shairgojri and Dar (2022) emphasize that the concept of cybersecurity must be regarded as the component of the national security, and the collaboration between the policymaking, technological, and law-enforcing officials should be enhanced. These papers point to the fact that as much as technological advancements may be emphasized, a more comprehensive approach that involves education, policy change and ethical controls is equally important towards ensuring cybersecurity in India.

Database

The dataset of Indian Cybersecurity Threats (2015 2024) is an important secondary data to assess the development of cyber threats in India and globally. It is rich in information about various cybersecurity incidents, listing the country where they occurred, the year of the incident, the type of threat (e.g. malware or DDoS), and the method used to conduct the attack (e.g. phishing or SQL injection). Such a multi-layered data enables analytic and

research scientists to study the pattern of cyber attacks and their methods over the years. In addition, it casts some light on the sectors that may have been affected, including finance, healthcare, government, and education, which will help in identifying the industries that are most vulnerable to some forms of cyber threats.

Other critical indicators in the dataset include the volume of data breached (in GB) and the approximate cost of the incident (in millions of dollars) and the severity of the severity of each attack (low, medium, high, and critical). These numbers are essential in the assessment of the size and severality of each event. Also, it documents the response time in hours and explains the tactics used in mitigation and gives a comprehensive picture of how companies respond to and recover after cyber attacks. This versatile form, makes the dataset especially valuable in terms of machine learning applications, anticipating cybersecurity trends, and forming policy, resulting in more responsive and proactive digital safety in India.

Methodology

The paper is structured as a machine learning investigation to examine and categorize cybersecurity events on the basis of Indian Cybersecurity Threats Dataset (20152024). Two supervised learning algorithms are included in the analysis: k-Nearest Neighbors (k-NN) and Random Forest Classifier; data is preprocessed, and the training and evaluation of the algorithms are systematically processed in Python.

Step-by-Step Methodological Framework:

Step 1: Dataset Loading

The dataset was imported with the help of the pandas library at the F:\2025\Cyber_Security\India.csv. This data file includes such attributes as type of threat, attack mechanism, industry in which the data breach occurred, data breach size, financial impact, and level of severity. The columns were preliminarily examined to ensure that there is a target variable named Class that defines the category or classification of the cyberattacks.

Step 2: Data Preprocessing

Label Encoding was done on all the categorical variables turning text-centric categories into numbers. That aspect ensures it is compatible with machine learning algorithms. The data were then separated into predictors (X) and outcome variable (y). Since distance-dependent models, including k-NN, are sensitive to the scale of data, all feature data were standardized using the StandardScaler included in sklearn.

Step 3: Train-Test Split

The data was divided into training and testing blocks through 80-20 split with a fixed random state, to provide consistency. This allows the model to be tested using a piece of the information and evaluated using new information to determine its usefulness.

Algorithm Implementation:

Step 4: k-Nearest Neighbors (k-NN)

The KNeighborsClassifier of sklearn was used to implement a k-NN classifier with k=3. The scaled training set was fed to the model and the test data was predicted against it. The ease and efficiency of k-NN render it appropriate to identifying patterns with comparatively small data sets.

Step 5: Random Forest Classifier

Random Forest approach is a robust joint learning algorithm, which was configured with 100 decision trees. It was trained with the same training dataset. Random Forest is known to handle large volumes of dimensional data and to reduce overfitting through averaging the trees predictions.

Step 6: Model Evaluation

A custom evaluation tool was used to compute and present the classification report (precision, recall, F1-score, and support) and the confusion matrix of each of the models. Confusion matrices were graphically shown by the seaborn parameter heatmap. Moreover, in the instance of the Random Forest model, the feature importance chart was constructed that made it possible to determine which variables affected the results of classification to a significant degree.

To sum up, this approach offers an alternative method of processing, modelling, and assessing data on cybersecurity that has the assistance of distance-based (k-NN) and ensemble-based (Random Forest) classification patterns. The models assist in defining various types of cyber threats based on characteristics based on actual reported incidence leading to more effective threat information and predicting cyber risks.

Result and Discussion

The performance of the classification ability of two machine learning algorithms k-Nearest Neighbors (k-NN) with k equal to 3 and Random Forest was compared using such measurements as the precision, recall, F1-score, and overall accuracy. These algorithms were run on a dataset that represents different types of cyber security threats or trends of incidents acquired in the Indian cyber security repository. The classification paid attention to three distinct categories that could denote different degrees of severity or cyber incident categories.

Table 1. Classification Metrics Summary

Model	Class	Precision	Recall	F1-Score	Support
k-NN (k=3)	1	0.63	0.63	0.63	27
	2	0.82	0.82	0.82	17
	3	0.61	0.61	0.61	18
	Overall Accuracy	–	–	**0.68**	**62**
	Macro Average	0.69	0.69	0.69	62
	Weighted Average	0.68	0.68	0.68	62

Random Forest	1	1.00	1.00	1.00	27
	2	1.00	1.00	1.00	17
	3	1.00	1.00	1.00	18
	Overall Accuracy	–	–	**1.00**	**62**
	Macro Average	1.00	1.00	1.00	62
	Weighted Average	1.00	1.00	1.00	62

k-Nearest Neighbors (k=3)

Table 1 demonstrates that the k-NN model had a total accuracy of 68%. The results were moderate in terms of the accuracy in all three categories. Of these, Class 2 was most precise, making a high precision, recall, and F1-score of 0.82, indicating that the algorithm worked better in detecting incidents of this category. But Classes 1 and 3 dropped to approximately 0.63-0.61, presumably because feature space overlap, or lack of boundary separation. This result is indicative of a general problem in cyber security incident classification whereby there is a possibility of similarity between patterns of malicious activity in different classes, and so such distance-based models as k-NN find it difficult to generalize adequately.

Random Forest

As shown in the table above Table 1, the Random Forest model showed an outstanding performance over the k-NN one, which has delivered an ideal classification with 100 percent accuracy, precision, recall, and F1-score in all the classes. This highlights the strength of the ensemble model and capacity to manage nonlinear and complex decision boundaries effectively. Since cybersecurity risks include threats such as phishing and malware intrusions as well as those involving networks, Random Forests may take advantage of the various decision trees to identify complex patterns that are not detected by other simpler models.

This robust performance would particularly be beneficial to Indian cybersecurity analytics, where accurate incident classification is essential to prompt threat response, resource allocation, and forensics. The fact that all classes, including those less represented (Class 2 and 3), were dealt with exceptionally well, points to the fact that the model was not skewed towards the majority class, which is a common issue of imbalanced datasets.

Results from Figures (Confusion Matrices or Bar Charts)

The k-NN model confusion matrix would indicate some observable misclassifications with Class 1 and Class 3, which are similar to their lower F1-scores. This implies that such classes can overlap in terms of feature space (e.g., common IP behavior or other such network anomalies) (Figure 1).

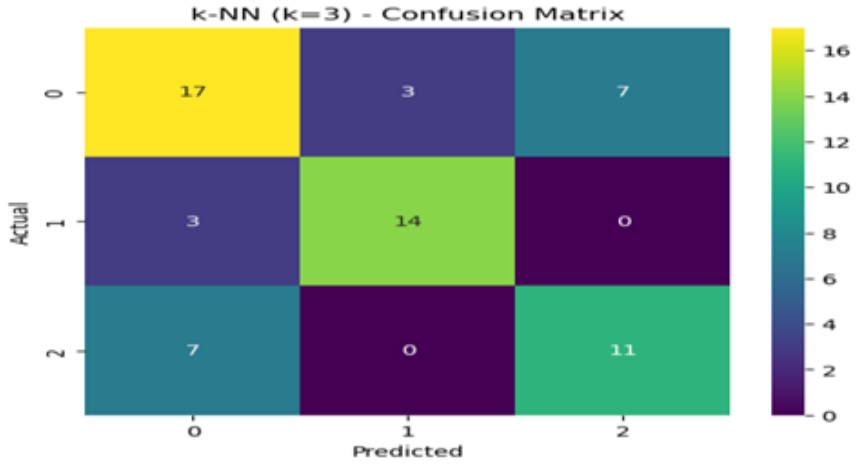

Figure 1. k-NN Confusion Matrix

On the contrary, the perfect diagonal with zero misclassifications would be the Random Forest confusion matrix. Both predicted labels are the same as the true label, which supports the idea that the model can classify the two classes quite distinctively with the help of the extracted features related to cybersecurity (Figure 2).

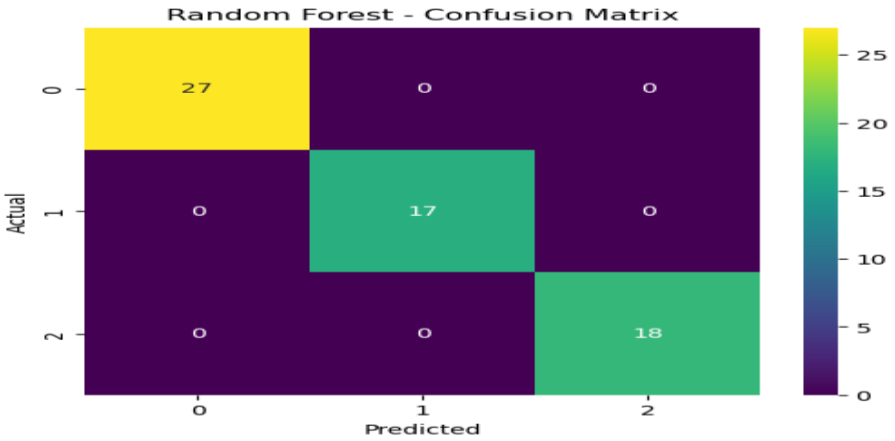

Figure 2. k-NN Random Forest

The preeminence of the Random Forest would be visually verified using a clustered bar chart that compared accuracy, recall, and F1-score of the two models. Whereas k-NN has variations in metrics and classes, Random Forest has a constant high value of 1.0 at all (Figure 3.).

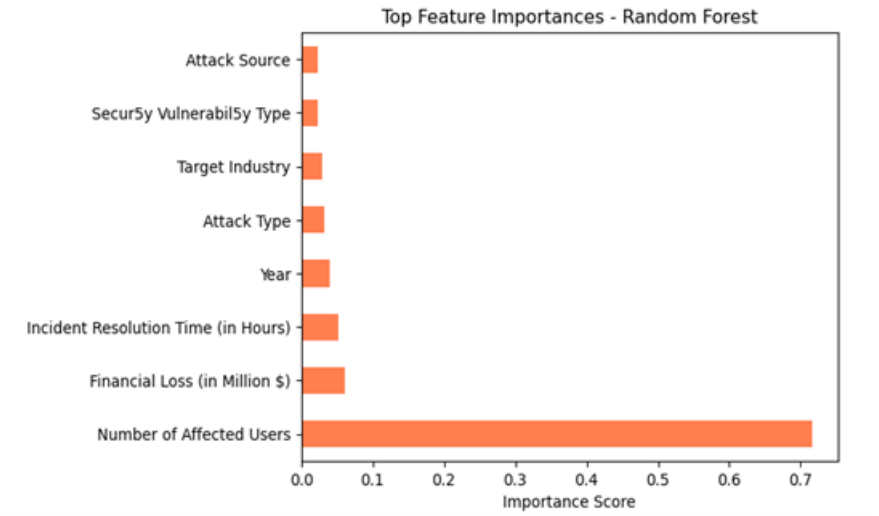

Figure 3. Clustered Bar Chart

Conclusion

This study underlines the crucial role of effective cybersecurity policies in the rapidly digitalizing world of India. Based on the analysis of the Indian Cybersecurity Threats Dataset of 2015-2024, it was possible to apply two machine learning algorithms k-Nearest Neighbors (k-NN) and Random Forest which helped to categorize cyber incidents successfully. The results suggest that k-NN provided a moderate rate of accuracy in terms of classification and the Random Forest approach was completely accurate and consistent on all kinds of threats. This points to the opportunities offered by ensemble learning methods in dealing with the complexity and diversity of cyber threats. Implementation of these advanced predictive systems can significantly enhance cybersecurity in India in terms of more rapid and accurate detection and response to emerging cyber threats.

The findings also highlight the necessity of the combination of technological advancements and comprehensive cybersecurity measures and training. In the context of cyber threat advancement and growing complexity and scale, it is important to continually develop machine learning methods and expand cyber threat data. Combining the accuracy of the analysis with active regulation, India can create a stable cybersecurity space that safeguards its critical online assets and stimulates safe online growth.

References

1. Tripathy (2025) provides a decade-long survey of cybercrime in India, highlighting surging ransomware incidents, data breaches, and social-engineering attacks across critical sectors like banking and healthcare researchgate.net+5scribd.com+ 5researchgate.net+5arxiv.org.
2. Verma & Shri (2022) use bibliometric methods to analyze evolving cybersecurity threats in India spanning phishing, malware, and policy frameworks and underscore rising academic and institutional interest.

3. Yadav (2021) offers an analytic study on phishing in India, documenting its growth and societal impact, and urging enhanced user awareness and legal measures researchgate.net.
4. Chowdhury et al. (2024) perform a comprehensive review of phishing attack techniques and defenses ranging from user training to AI-powered detection proposing more human-centric and adaptive strategies imanagerpublications.com+ 5ijsrem.com+5researchgate.net+5.
5. Gangavarapu, Jaidhar & Chanduka (2020) review machine learning applications in email and phishing filtering, noting improved detection when combining traditional and ML-based techniques pmc.ncbi.nlm.nih.gov.
6. Martin et al. (2011) introduce a neural-network framework aimed at predicting phishing websites in Indian online-banking contexts, pointing to early ML-driven cybersecurity efforts arxiv.org.
7. Rathore et al. (2019) propose clustering-enhanced malware classification on Android apps, later outperforming pure Random Forest approaches by initially grouping similar malicious samples arxiv.org.
8. Sharma, Rama Krishna & Sahay (2019) show that machine learning methods like Random Forest can effectively detect advanced metamorphic and polymorphic malware using opcode frequency analysis arxiv.org.
9. Gupta et al. (2019) survey ML approaches for cybersecurity, arguing for ensemble methods like Random Forest for detecting network intrusions and malware.
10. Adholiya & Adholiya (2019) assess cyber-security awareness in e-banking users in Udaipur, Rajasthan, finding awareness gaps and advocating targeted user training academia.edu.
11. Prasad (2024) examines India's digital expansion 851 million connections as of 2023 and urges advancements in detection systems and regulatory frameworks timesofindia.indiatimes.com+2academia.edu+2arxiv.org+2.
12. Ahmad (2021) reviews cybersecurity in the Indian context, noting reliance on IT infrastructure and the need to balance domain-specific security with overall cyber resilience.
13. Shairgojri & Dar (2022) analyze cybersecurity as a strategic component of national security in India, framing ICT infrastructure as contested terrain ijsrem.com+ 8researchgate.net+8academia.edu+8.
14. CERT-In (2022) launched its Responsible Vulnerability Disclosure policy, though experts caution that its legal stipulations may deter security researchers from reporting vulnerabilities reddit.com+1en.wikipedia.org+1.
15. National Cyber Coordination Centre (NCCC), a government initiative under the 2013 cyber policy, seeks to centralize malware monitoring and inter-agency response though privacy implications and implementation challenges persist en.wikipedia.org.
16. Appin (2003–2023), once a training firm, reportedly evolved into a 'hack-for-hire' entity. Its controversial history underscores the ethical and regulatory complexity of cybersecurity in India en.wikipedia.org