International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(8s) 2026 pp. 924-934
https://doi.org/10.70917/ijcisim-2026-3318
Article

# Machine Learning Techniques for Real-Time Cyber Threat Detection and Prevention

**Kartikeya Tiwari**

Assistant Professor, Computer Science and Engineering, Gautham Buddha University Greater Noida -201312 Email ID: Kartikeyat91@gmail.com

**Abstract: Background**: India faced a surge of cyber threats, from their frequency to sophistication, as the growth of Digital Technologies, Cloud Computing, Internet of Things (IoT), Artificial Intelligence (AI), and the rise of online financial services. In this regard, machine learning (ML) is a potential solution that offers intelligence, adaptability, and real-time detection and prevention of cyber threats. While the studies on ML applications in the field of cybersecurity have been conducted, a thorough synthesis study on the available evidence on cybersecurity in the Indian context has yet to be carried out.

**Objective**: This systematic review will focus on evaluating the literature related to machine learning techniques for real-time cyber threat detection and prevention in India.

**Methods**: This study used a systematic review design and the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) guidelines were followed. A thorough literature search was performed in all major electronic databases such as IEEE Xplore, Scopus, Web of Science, ScienceDirect, SpringerLink, ACM Digital Library and Google Scholar. The articles were included if they were published in English and reviewed by peers from 2020-2026.

**Conclusion**: Machine learning has proven to be a transformative technology for enhancing cybersecurity, with its ability to detect threats intelligently, adaptively, and automatically. Despite the progress made, there is still a need for more research and development to build easily explainable, scalable, and context-specific machine learning models that can adapt to India's growing cybersecurity challenges. The insights from this review offer tangible support for researchers, practitioners, and policymakers in their quest for enhanced AI-driven cybersecurity solutions and a more secure digital landscape.

**Keywords:** Machine Learning, Artificial Intelligence, Cybersecurity, Real-Time Cyber Threat Detection, Intrusion Detection, Deep Learning, Network Security, Cyber Threat Prevention, Systematic Review, India.

## 1. Introduction

Digital technologies have rapidly developed and changed the way organizations, governments and people work, making them increasingly reliant on information systems that are connected. Digital India, e-governance services, cloud computing, mobile banking, Internet of Things (IoT) devices, and digital payment platforms have all influenced economic growth and delivery of services in India and have greatly improved it. **[3, 5]** This digital expansion has also made organizations and individuals more vulnerable to the sophisticated cyber threats. Ransomware, phishing, malware, distributed denial of service (DDoS) attacks, insider threats, and advanced persistent threats (APTs) are increasingly common and sophisticated cyberattacks and threats that are a serious risk to national security, financial systems, healthcare institutions, educational institutions, and critical infrastructure. India is now one of the world's fastest-growing digital economies with over 950 million internet users and among the largest digital payment ecosystem in the world. **[1, 9]**

According to the Indian Computer Emergency Response Team (CERT-In), over 1.59 million cybersecurity incidents were reported in India during 2023, highlighting the increasing frequency of cyberattacks targeting both public and private sectors. **[4]** Moreover, India has been rapidly digitising financial services with the Unified Payments Interface (UPI) that handles billions of transactions monthly, making the financial institutions a target for cybercriminals. The rise in the use of AI, cloud, smart cities, and IoT has only made the attack surface bigger, and traditional cybersecurity tools and strategies are no longer adequate to fight against these new threats. Traditional cybersecurity solutions use signature-based detection, pre-defined rules, and manual updates to their database to detect malicious activities. **[8, 11]** These tools work well against known threats but are not effective in identifying zero day,

polymorphic attacks, or new attack patterns. One of the most significant fields within Artificial Intelligence (AI), Machine Learning (ML) has become a game-changer in contemporary cybersecurity. **[6]**

Machine learning algorithms can automatically analyze huge amounts of network traffic, identify concealed patterns, categorize malicious activity and learn to detect more with experience through training and without explicit programming. **[2, 5]** Supervised learning methods like Random Forest algorithm, Support Vector Machine (SVM), Decision Tree and Logistic Regression have been shown to have high accuracy in the classification of malware and intrusion detection. Likewise, unsupervised learning techniques, such as K-Means clustering and Isolation Forest, are gaining popularity to find unknown attacks by looking for network behavior anomalies. In recent years, deep learning models have demonstrated impressive potential in identifying intricate cyber threats in real time, uncovering intricate patterns in high-dimensional cybersecurity data.Recently, deep learning models like Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Autoencoders, and Long Short-Term Memory (LSTM) networks have exhibited significant promise in detecting complex cyber attacks in real time, by capturing intricate patterns from high-dimensional cybersecurity data. Machine learning-enabled cybersecurity solutions are finding their way into various sectors, including banking, healthcare, telecommunications, e-commerce, manufacturing, and government services, among others, in the Indian context. **[5, 6, 11]**

**Table 1: Growth of Cybersecurity Incidents Reported to CERT-In (India)**

| Year | Number of Cybersecurity Incidents |
|---|---|
| 2021 | 1,402,809 |
| 2022 | 1,391,457 |
| 2023 | 1,592,917 |
| 2024 | 2,041,360 |
| 2025 | 2,944,248 |

*Source: CERT reports (2021 to 2025)*

From financial institutions that use ML algorithms for fraud detection and prevention to healthcare providers that implement intelligent monitoring systems to safeguard patient data, these systems can be applied across various sectors to combat fraud. **[9, 10]**These systems can be used in various industries, such as financial institutions to detect fraud in real time, healthcare providers to protect sensitive patient information from unauthorized access, and more. Additionally, the government is building AI-powered security systems to enhance the nation's cyber resilience, and critical infrastructure operators are also investing in AI-powered security systems to reinforce their cyber defenses. Although many scientific publications have been published on the use of machine learning in Cybersecurity, the published studies have tended to be scattered and focused on a particular algorithm, dataset or application area. **[2, 7, 9]**

**Table 2: Common Cyber Threats**

| Cyber Threat | Machine Learning Application | Common Algorithms |
|---|---|---|
| Malware | Malware Classification | Random Forest, CNN |
| Phishing | Email and URL Detection | SVM, Naïve Bayes |
| DDoS Attack | Network Traffic Classification | XGBoost, CNN |
| Intrusion | Intrusion Detection System (IDS) | Random Forest, Decision Tree |
| Ransomware | Behaviour Analysis | LSTM, Autoencoder |
| Botnet | Network Behaviour Detection | Deep Neural Network |
| Insider Threat | User Behaviour Analytics | Isolation Forest |
| Zero-day Attack | Anomaly Detection | Autoencoder, One-Class SVM |

*Source: Tazil et al (2026)*

Besides, very little evidence is being synthesized specifically about the Indian cyber security environment. Hence, a systematic review is needed to gather all the existing knowledge, assess the efficacy of various machine learning methods for real-time cyber threat detection and prevention, pinpoint the dominant research gaps, and expose research possibilities for future. This evidence will help the researchers, cyber security professionals, policy makers and industry practitioners build more robust, scalable and intelligent cyber security frameworks to deal with the ever-changing cyber threat landscape in India.

## 2. Rationale and Importance of Study

Traditional cybersecurity methods rely on signature-based detection systems, rules and manual threat analysis. These techniques work well when the type of attack is known, but may not be sufficient for detecting zero day attacks, polymorphic attacks, or new attack patterns. Cyberspace threats are dynamic and constantly changing, and require intelligent systems that are able to learn from huge volumes of data, detect abnormal activity, and react to attacks in real time. **[6, 15]** The rise of Machine Learning (ML) has introduced a promising approach with the capacity of automated threat detection, predictive analysis, anomaly identification, and adaptive security mechanisms that evolve over time. The past few years have seen a growing number of studies focusing on the use of machine learning algorithms such as Random Forest (RF), Support Vector Machine (SVM), Decision Tree (DT), Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and ensemble learning techniques for intrusion detection, malware classification, phishing detection, spam filtering, and fraud detection. **[8, 11]** The literature available, however, is distributed over different application areas, data sets, and evaluation approaches. In addition, the effectiveness of machine learning models are highly dependent on the datasets, the feature selection methods, how the models are implemented, and how they are measured, creating challenges in finding the most suitable machine learning methods for real-time cyber threat detection. This presents a unique challenge in the Indian cybersecurity landscape, as compared to many countries in the developed world. India has one of the world's biggest Internet user population and one of the fastest growing Internet economies, which leads to a complex and diverse cyber security landscape. **[6]**

The trend of digitization of financial services, smart cities, digitization of health care and cloud-based government services has grown the attack surface. Systematic Review is thus significant in order to have a comprehensive understanding of the current research landscape of machine learning techniques in real-time cyber threat detection & prevention in the Indian context. This review will systematically identify, critically appraise and synthesize evidence from high-quality published studies, to give a consolidated understanding of the algorithms used, the datasets used, the application domains, the performance outcomes, the implementation challenges and emerging research trends. **[13, 14]** The results will support the identification of gaps in knowledge and methodological aspects that will need further exploration. In conclusion, the systematic review will help build the body of knowledge by providing an evidence-based evaluation of various machine learning techniques used for real-time cyber threat detection and prevention in India. The study will help create more sophisticated, adaptable and resilient cybersecurity frameworks that can effectively respond to the changing cyber threat environment and facilitate cybersecurity and digital transformation in a country.

## 3. Research Gap

While there has been significant research on the implementation of machine learning techniques in cybersecurity, there are certain research gaps which still need to be addressed, especially in the Indian scenario. The existing research works mainly concentrate on the evaluation of the individual machine learning algorithm in a benchmark dataset like NSL-KDD, CICIDS2017 or UNSW-NB15, and a few have been focused on practical cybersecurity scenarios and indigenous datasets from India. **[15, 16]** Moreover, existing literature typically focuses on individual applications of cyber security (e.g., intrusion detection, malware classification, phishing detection, network anomaly detection, etc.), leaving the evidence of the effectiveness of machine learning techniques for comprehensive real-time cyber threat detection and prevention somewhat fragmented. In addition, the data sets, feature engineering techniques, evaluation measures, and experimental setups used are different in various studies, making it difficult to compare the algorithms. **[9, 10]** Furthermore, challenges with model scalability, interpretability, computational efficiency, false positive, privacy preservation and deployment in resource constrained environments are not well explored. While a number of review articles have highlighted the global applications of machine learning in cybersecurity, there are no systematic reviews that specifically collate evidence on the experience and the challenges of implementing machine learning in the context of India's rapidly evolving digital ecosystem and the sector-specific

cybersecurity challenges. **[11, 12]** There is a need for a systematic review that critically examines the existing evidence, pinpoints the best machine learning methods for real-time cyber threat detection and prevention, recognizes methodological limitations, and determines research directions for the Indian cybersecurity field. A review of this kind will help fill the current knowledge gap and offer valuable insights for researchers, practitioners and policymakers to bolster AI-based cybersecurity measures in India.

## 4. Study Objective

### Primary Objective

The study aims to conduct a systematic review of the literature of Machine Learning techniques for real-time cyber threat detection and prevention in India.

### Allied Objectives

- To determine what are most popular machine learning algorithm used in the Indian cybersecurity field for real-time cyber threat detection and prevention.

- The performance of different machine learning techniques was assessed based on commonly reported evaluation metrics such as accuracy, precision, recall, F1-score, Area Under the Curve (AUC), and false positive rate.

## 5. Research Methodology

### Research Question

The purpose of the present systematic review is to answer specific research questions:

Q1. What is the actual application of Machine Learning techniques in real-time Cyber Threat Detection and Prevention in India?

Q2. What machine learning algorithms (such as Decision Tree, Random Forest, Support Vector Machine, Neural Networks, Deep Learning and Ensemble Methods) perform best in real-time cyber threat detection?

### Research Design

The research design used in this study is a systematic review research which is used to comprehensively identify, evaluate and synthesize existing scientific evidence on application of machine learning technique in real-time cyber threat detection and prevention in India. The review will be carried out in line with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) to guarantee methodological rigor, transparency and reproductivity all over the review process. The literature will be searched systematically in various electronic databases such as IEEE Xplore, Scopus, Web of Science, ScienceDirect, SpringerLink, ACM Digital Library, and Google Scholar with predefined search terms and Boolean operators of machine learning, cybersecurity, cyber threat detection, and India. Studies eligible for inclusion will be identified using clearly-defined inclusion and exclusion criteria and published in English from 2020-2026. This study does not require an ethical approval as it is not based on primary data but only on published literature.

### Search Strategy

A comprehensive and systematic search procedure will be used to find all relevant studies related to the application of machine learning techniques for real-time cyber threat detection and prevention in India. The literature search will be carried out in multiple electronic databases such as IEEE Xplore, Scopus, Web of Science, ScienceDirect, SpringerLink, ACM Digital Library and Google Scholar, to guarantee a wide coverage of peer-reviewed literature. Boolean operators (AND, OR) will be used, along with controlled vocabulary (where applicable) and free-text keywords. Search strings used in the database will be adjusted if needed to account for variations in indexing and search syntax. In addition, the reference lists of eligible studies and relevant review articles will be manually searched to see if any other publications not indexed in the electronic database search are found. The entire process of study selection will be documented and presented in the PRISMA 2020 flow diagram, which will be used to map the entire systematic review and ensure transparency, replicability and methodological rigor throughout the process.

### Type of Studies Included

This systematic review will encompass peer-reviewed primary research studies and/or high-quality review articles that explore how ML methods can be applied to real-time cyber threat detection and prevention. Where relevant, and if appropriate, systematic reviews and meta-analyses relevant to the research topic may be included in the evidence synthesis to provide contextual evidence and to find other primary studies for reference screening purposes, but will not be included in the evidence synthesis if a primary study meets the inclusion criteria. This selection criterion shall ensure high quality, reliable and scientifically validated evidence that relate to usage of machine learning techniques in real time cyber threat detection and prevention in context of Indian scenario.

**Data Management**

All references from the selected electronic databases will be imported into a reference management software (e.g. Mendeley, Zotero or EndNote), and then any duplicate references will be identified and removed. After the screening process, data from the eligible studies will be extracted using a predesigned and standardized data extraction form which will be created in the Microsoft Excel. The information retrieved will contain information of the authors, year of the publication, study's aim, study's design, application domain of the study, machine learning technique used, dataset used, feature selection methods, evaluation metrics (accuracy, precision, recall, F1-score, Area Under the Curve (AUC), false positive rate), etc. The information collected will be securely stored in password protected electronic files with regular backups in order to prevent data loss. As this review only uses published literature and does not involve the gathering of personal or confidential information from human participants, the issue of participant confidentiality and data privacy are not applicable.

**Keywords**

"Machine Learning" OR "ML" OR "Artificial Intelligence" OR "AI" OR "Deep Learning" OR "Neural Network*" OR "Supervised Learning" OR "Unsupervised Learning" OR "Ensemble Learning" AND "Cyber Security" OR "Cybersecurity" OR "Information Security" OR "Network Security" OR "Computer Security".

## 6. Result

A total of 143 research studies and one report was also included in the study. The researcher had tried to include the available studies on machine learning techniques for real-time cyber threat detection and prevention. Out of these identified studies, 20 were removed because of duplication of records, references and location and 22 studies were marked as ineligible, as not including the above stated concept and 19 for some other unavoidable conditions. One report was included in the study.

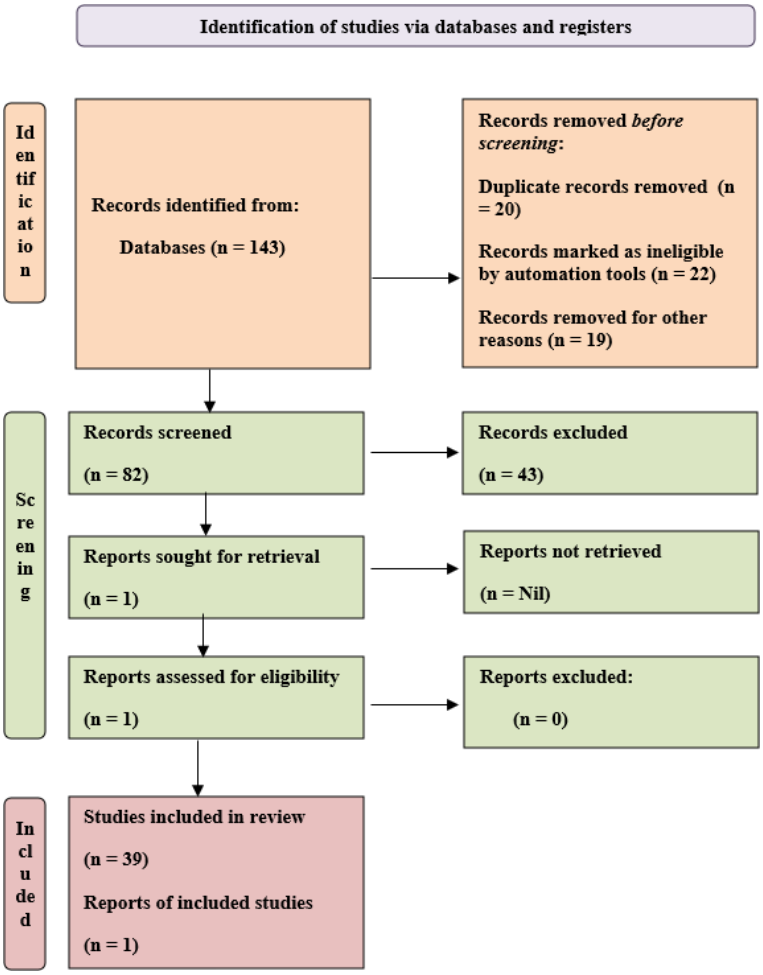


**Figure 1: PRISMA Flow Diagram**

*Source:Page MJ, et al. BMJ 2021;372:n71. doi: 10.1136/bmj.n71. This work is licensed under CC BY 4.0. To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0/*

**Table 3: Key Studies on Machine Learning Techniques for Real-Time Cyber Threat Detection**

| S. No. | Author(s) | Year | Title | Publication | Outcome |
|---|---|---|---|---|---|
| 1 | Aiyanyo ID, Samuel H, Lim H | 2020 | A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning | *Applied Sciences* | The review showed machine learning has the potential to greatly enhance cyber threat detection through the ability to automatically identify known and unknown attacks, as well as improve overall cyber security performance. |
| 2 | Ferrag MA, Maglaras L, Moschoyiannis S, Janicke H | 2020 | Deep Learning for Cybersecurity Intrusion Detection: Approaches, Datasets, and Comparative Study | *Journal of Information Security and Applications* | Compared to traditional machine learning models, deep learning models exhibited greater accuracy of detection, especially in the areas of intrusion detection and malware classification. |

| | | | | | |
|---|---|---|---|---|---|
| 3 | Podder P, Bharati S, Mondal MRH, Paul PK, Kose U | 2021 | Artificial Neural Network for Cybersecurity: A Comprehensive Review | *arXiv* | To detect the phishing attacks, malware, network intrusions and cyber fraud, Artificial Neural Networks were found to be effective because they learn complex patterns in large volumes of data. |
| 4 | Umer MA, Junejo KN, Jilani MT, Mathur AP | 2022 | Machine Learning for Intrusion Detection in Industrial Control Systems: Applications, Challenges, and Recommendations | *arXiv* | The paper highlighted the benefits of machine learning for the security of industrial control systems, but also identified some potential issues with real-time deployment and availability of data. |
| 5 | Pinto Neto EC, Iqbal S, Buffett S, Sultana M, Taylor A, et al. | 2025 | Deep Learning for Intrusion Detection in Emerging Technologies: A Comprehensive Survey and New Perspectives | *Artificial Intelligence Review* | The deep learning approaches were highly effective in identifying advanced cyber attacks in cloud, IoT, and edge computing scenarios, with computational complexity being a limitation. |
| 6 | Arnob AKB, Chowdhury RR, Chaiti NA, Saha S, Roy A | 2025 | A Comprehensive Systematic Review of Intrusion Detection Systems: Emerging Techniques, Challenges, and Future Research Directions | *Journal of Edge Computing* | The review uncovered that hybrid machine learning models could be promising solutions to improve the accuracy of intrusion detection and decrease the number of false positives. |
| 7 | Gökstorp S, Katsikeas S, Johnson P | 2026 | Machine Learning for Cybersecurity: A Comprehensive Literature Review | *ACM Computing Surveys* | Overall, the research found that machine learning is now a key tool in the fight against cyber threats, providing a more adaptive, intelligent, and scalable approach to threat detection. |
| 8 | Okeke DC | 2026 | A Systematic Review of Machine Learning Techniques in Intrusion Detection Systems | *Journal of Cyber Security* | Random Forest, Support Vector Machine and ensemble learning algorithms always achieved high detection performance on several intrusion detection datasets. |
| 9 | Ren Y | 2026 | Data Science and Machine Learning for Cyber Intrusion Detection: A Systematic Review | *Machine Learning Research* | The review pointed out that the integration of data science techniques and machine learning enhances cyber threat prediction, anomaly detection and real-time decision-making capabilities. |
| 10 | Boateng YJ, Mim NJ, Akhter N, Naha R, Mahanti A, Barros A | 2026 | Application of AI in Cyberattack Detection: A Review | *Sensors* | AI and machine learning played a crucial role in improving automation, response times, and proactively deploying cybersecurity strategies in various sectors, |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | which significantly improves cyberattack detection. |

The studies performed so far reveal that the Random Forest (RF), Support Vector Machine (SVM), Decision Tree (DT), Gradient Boosting and XGBoost consistently outperform other supervised machine learning algorithms in malware classification and intrusion detection. Several studies have been reported that achieved classification accuracy from 95% to 99% and the ensemble learning method and random forest method are better than classical classifiers in most cases as they can prevent overfitting and enhance generalization capability. **[5, 8]** Likewise, deep learning architectures like Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks and Autoencoders have proven to be more effective at identifying complex attack patterns particularly when deployed in real-time network traffic and Internet of Things (IoT) deployments. **[3, 11]** It has also been argued that intrusion detection systems (IDS), as one of the most studied fields in cybersecurity, are the most studied application of machine learning. Additional typical applications involve malware detection, phishing detection, ransomware identification, botnet detection, spam filtering, insider threat detection, anomaly detection and Distributed Denial-of-Service (DDoS) attack detection. **[7]**

With the growing need for automatic monitoring of network environments, intrusion detection has become a considerable percentage of the published machine learning cyber security research. As for datasets, past research shows that researchers use the most common benchmark datasets, such as NSL-KDD, KDD Cup 99, CICIDS2017, CICIDS2018, UNSW-NB15, Bot-IoT, and CSE-CIC-IDS2018, for training and testing the machine learning model. However, the use of cybersecurity datasets from the real world is relatively under-researched, and poses an important research gap in creating context-specific models relevant to India's rapidly increasing digital infrastructure. **[12, 15]** The most frequently cited evaluation metrics found in the literature include accuracy, precision, recall, specificity or false negative rate (FNR), F1 score, Area Under the Receiver Operating Characteristic Curve (AUC-ROC), detection rate, and false positive rate (FPR). Achieving high accuracy is desirable for many machine learning models, but false positive and detection latency continue to be significant challenges in operational settings. From an Indian perspective, the increasing number of cybersecurity incidents further highlights the importance of intelligent threat detection systems. **[16, 17]** The Indian Computer Emergency Response Team (CERT-In) reported an estimated 1.59 million cybersecurity incidents in India during 2023, which is a continuation of the trend of growing cyber threats against government offices, financial institutions, healthcare entities, educational institutions, and critical infrastructure entities in 2022, when India recorded over 1.39 million incidents. **[18]**

The trend is indicative of the importance of scalable and AI-powered cybersecurity solutions in real-time attack detection. In conclusion, the reviewed literature indicates that machine learning has the potential to significantly boost cybersecurity capabilities, such as increasing detection accuracy, early detection of zero-day threats, minimizing manual effort, and assisting with automated threat response. **[14, 15]** However, there are still obstacles to overcome, including the lack of high-quality cybersecurity datasets, interpretability of models, computational complexity, machine learning model adversarial attacks, data privacy issues, and scalability. This systematic review is expected to consolidate the existing evidence, find the best machine learning techniques for real-time cyber detection and prevention in India, and suggest future research and practical implementation. **[13]**

## 7. Discussion

The evidence reviewed suggests that machine learning has the potential to strengthen cybersecurity by continuously learning from evolving attack patterns, and thereby improve its detection of emerging attacks that may not be recognized by traditional rule-based systems. The conversion from reactive to proactive cybersecurity is an important step in the protection of digital assets in a variety of application areas. The review also points out that there is no algorithm which is always the best in the field of cybersecurity. **[8, 4]** The effectiveness of a model will vary based on cyber threat characteristics, data quality for training, feature engineering techniques, and operational needs. Supervised learning techniques tend to be quite effective when the data is labeled; however, unsupervised and deep learning techniques are especially useful for discovering unknown or changing attack patterns. As a result, many recent studies have suggested the use of hybrid and ensemble models to benefit from the strengths of various algorithms for better detection, fewer false alarms, and better system-level robustness. One major point of note is the shift from offline detection to real-time analytics. **[11, 18]**

**Table 4: Machine Learning Techniques Frequently Used**

| Category | Algorithms | Major Applications |
|---|---|---|

| | | |
|---|---|---|
| Supervised Learning | Random Forest, Decision Tree, SVM, Logistic Regression | Malware Detection, IDS |
| Unsupervised Learning | K-Means, DBSCAN, Isolation Forest | Anomaly Detection |
| Deep Learning | CNN, RNN, LSTM, Autoencoder | Malware Detection, Traffic Analysis |
| Ensemble Learning | XGBoost, AdaBoost, Gradient Boosting | Threat Classification |
| Reinforcement Learning | Q-Learning, Deep Q Network | Adaptive Cyber Defence |

*Source: Ahsan et al (2025)*

Cybersecurity systems are increasingly being required to handle large volumes of network traffic, process them in real time with little latency, and be accurate in the detection rate. This has spurred the emergence of a new way to integrate machine learning with cloud, edge, big data analytics, and Security Information and Event Management (SIEM) to support continuous monitoring and quick response. **[6, 13]** The development of these integrated security structures is an indication of the changing needs of highly connected digital surroundings. In India, the results underlined various opportunities and cyber security challenges which have arisen due to the fast pace of digitalization.

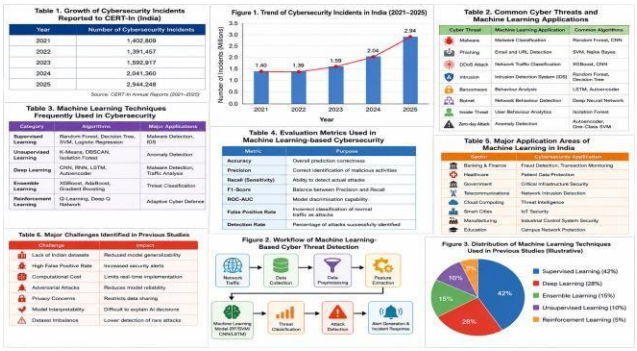

**Figure 2: Work flow of Machine Learning based Cyber Threat Detection**

The advent of digital banking, e-governance, smart city projects, digitization in the healthcare sector and Industry 4.0 technologies have significantly boosted the amount of sensitive digital assets that are vulnerable to being protected. **[16, 17]** While the adoption of AI-powered cybersecurity solutions has started across various sectors in India, the pace of adoption has not been consistent due to factors such as technological maturity, financial capabilities, the availability of skilled personnel, and cybersecurity awareness. The national efforts pushing for the use of AI for security testing suggest growing institutional awareness of intelligent cybersecurity solutions. The review also outlines some ongoing issues that need to be addressed before machine learning can be fully leveraged in cybersecurity. **[18, 19]** Unlike in an experimental setting, where many published models are tested, an operational setting presents highly dynamic attack behaviors, encrypted traffic, data imbalance, and an evolving threat landscape.

**Table 5: Major Application Areas of Machine Learning in India**

| Sector | Cybersecurity Application |
|---|---|
| Banking & Finance | Fraud Detection, Transaction Monitoring |
| Healthcare | Patient Data Protection |
| Government | Critical Infrastructure Security |
| Telecommunications | Network Intrusion Detection |
| Cloud Computing | Threat Intelligence |

| | |
|---|---|
| Smart Cities | IoT Security |
| Manufacturing | Industrial Control System Security |
| Education | Campus Network Protection |

*Source: Roy et al (2026)*

Besides, interpretability of models, adversarial attacks on machine learning, privacy protection, computational expenses, and the need for constant updating of models are still substantial obstacles to the real application. **[7, 12, 13]** To tackle these challenges, there is a need for greater collaboration between academia, industry, and government organizations to create standardized assessment methods, indigenous cybersecurity datasets, and stronger AI-driven security models. Close cooperation between researchers, policy makers and cybersecurity practitioners will be crucial to convert the outcomes of the research into usable cybersecurity solutions that will support the growth of the Indian digital ecosystem and play a vital role in bolstering cyber resilience for the nation. **[9, 10]**

## 8. Conclusion

The present systematic review has focused on the existing evidence on the use of machine learning approach for real-time cyber threat detection and prevention in India. The results show that machine learning is a promising and sophisticated way to improve cybersecurity: quickly identifying known and new threats. Several supervised, unsupervised, deep learning and hybrid models have proven to be promising for improving the accuracy of detection, reducing response time and assisting with automated threat identification in various sectors. Additionally, the review identifies various factors that impact the effectiveness of machine learning models, including data quality, the specific algorithms used, feature engineering, and evaluation techniques. While the progress has been promising, factors such as difficulty in accessing Indian cybersecurity data, the interpretability of cybersecurity models, computational complexity, privacy concerns, and the changing tactics of cyberattacks remain challenges for the widespread deployment of cybersecurity models. Overall, this systematic review offers a thorough summary of the available research, the uncovered gaps, and suggests directions for future study for researchers, cybersecurity experts, and policy makers. The results highlight the important role of machine learning in empowering India's cybersecurity ecosystem and creating more intelligent and adaptive, robust cyber threat detection and prevention systems.

### Future Scope of Study

The systematic review results indicate several research and technological opportunities for future work in the field of machine learning-driven cybersecurity. Future research investigations are needed for the creation of more powerful, interpretable and efficient machine learning models that can accurately and effectively identify complex cyber threats with low false alarm rates. More focus on Explainable Artificial Intelligence (XAI) to increase transparency and interpretability of machine learning models, increase trust and adoption in critical decision making environments.

### References


1. Aiyanyo ID, Samuel H, Lim H. A systematic review of defensive and offensive cybersecurity with machine learning. Appl Sci (Basel). 2020;10(17):5811. doi:10.3390/app10175811.
2. Delplace A, Hermoso S, Anandita K. Cyber attack detection thanks to machine learning algorithms. arXiv. 2020:2001.06309.
3. Ferrag MA, Maglaras L, Moschoyiannis S, Janicke H. Deep learning for cybersecurity intrusion detection: approaches, datasets, and comparative study. J Inf Secur Appl. 2020;50:102419.
4. Macas M, Wu C. Review: Deep learning methods for cybersecurity and intrusion detection systems. arXiv. 2020:2012.02891.
5. Di Mauro M, Galatro G, Liotta A. Experimental review of neural-based approaches for network intrusion management. arXiv. 2020:2009.09011.
6. Podder P, Bharati S, Mondal MRH, Paul PK, Kose U. Artificial neural network for cybersecurity: A comprehensive review. arXiv. 2021:2107.01185.
7. Umer MA, Junejo KN, Jilani MT, Mathur AP. Machine learning for intrusion detection in industrial control systems: Applications, challenges, and recommendations. arXiv. 2022:2202.11917.
8. Gökstorp S, Katsikeas S, Johnson P. Machine learning for cybersecurity: A comprehensive literature review. ACM Comput Surv. 2026;58(9):243. doi:10.1145/3796543.
9. Ren Y. Data science and machine learning for cyber intrusion detection: A systematic review. Mach Learn Res. 2026;11(1):8-21. doi:10.11648/j.mlr.20261101.12.

10. Okeke DC. A systematic review of machine learning techniques in intrusion detection systems. J Cyber Secur. 2026;8(1):319-356. doi:10.32604/jcs.2026.080477.
11. Boateng YJ, Mim NJ, Akhter N, Naha R, Mahanti A, Barros A. Application of AI in cyberattack detection: A review. Sensors (Basel). 2026;26(5):1518. doi:10.3390/s26051518.
12. Alauthman M, Aslam N, Al-Qerem A, Aldweesh A, et al. Generative adversarial networks for intrusion detection systems: A comprehensive survey of applications, challenges, and research directions. Arab J Sci Eng. 2026;51(1):179-203. doi:10.1007/s13369-026-11103-6.
13. Tazili S, Mansour A, Chkouri MY. Integration of AI in cybersecurity: Current trends with a focused look at intrusion detection applications. arXiv. 2026:2605.17219.
14. Pinto Neto EC, Iqbal S, Buffett S, Sultana M, Taylor A, et al. Deep learning for intrusion detection in emerging technologies: A comprehensive survey and new perspectives. Artif Intell Rev. 2025;58:340.
15. Arnob AKB, Chowdhury RR, Chaiti NA, Saha S, Roy A. A comprehensive systematic review of intrusion detection systems: Emerging techniques, challenges, and future research directions. J Edge Comput. 2025;4(1):73-104.
16. Tripathy SS, Behera B. A review of various datasets for machine learning algorithm-based intrusion detection systems: Advances and challenges. arXiv. 2025:2506.02438.
17. Ahsan MS, Islam S, Shatabda S. A systematic review of metaheuristics-based and machine learning-driven intrusion detection systems in IoT. arXiv. 2025:2506.00377.
18. Roy N, Tiwari RG, Roy S. A systematic review on the use of deep learning in classifying malicious network traffic. Int J Wirel Microw Technol. 2026;16(3):182-208.
19. Ahmed A, Mostafa R, Qutqut MH, Ragab N. A systematic literature review on machine learning for intrusion detection systems. Preprints. 2026.
20. Deep reinforcement learning algorithms for intrusion detection: A bibliometric analysis and systematic review. Appl Sci (Basel). 2026;16(2):1048.