myresearchgo Volume 2, Issue 5, May 2026, ISSN: 3107-3816 (Online)

Intelligent Cyber Attack Detection and Monitoring: A Comprehensive Review for Next-Generation Cybersecurity

Ms. Sonali A. Nanhe
PG Scholar
Department of Information Technology
Tulsiramji Gaikwad-Patil College of Engineering & Technology, Nagpur, India

Dr. Zeba Shaikh
Project Guide
Department of Information Technology
Tulsiramji Gaikwad-Patil College of Engineering & Technology, Nagpur, India

Prof. Nilesh Nagrale
Project Co-Guide
Department of Information Technology
Tulsiramji Gaikwad-Patil College of Engineering & Technology, Nagpur, India

Abstract- Cybersecurity professionals primarily focus on assessing risk profiles and developing strategies to mitigate them effectively. A key goal in this domain is to design robust methods that strengthen security measures. The integration of machine learning has significantly enhanced modern cyber defense systems. Breakthroughs in storage capacity, computing power, and networking have accelerated the adoption of cloud services, advanced networks, and evolutionary programming. As digital transformation accelerates worldwide, the demand for addressing complex privacy and security challenges grows rapidly, requiring stronger safeguards against emerging threats. Increasing vulnerabilities in computer systems have contributed to a rise in global cyber terrorism. By leveraging machine learning techniques, various global cybersecurity challenges—such as detecting malware, identifying ransomware, recognizing fraudulent activities, and verifying spoofing attempts—are being tackled more effectively. This review explores how online behavior modeling can be used for both attack and defense purposes, offering insights into cyber risks through machine learning tools and methodologies. It examines the most common cybersecurity threats and highlights how machine learning supports the detection and prevention of attacks, vulnerability analysis, and open-source risk evaluation in the digital landscape.

Keywords— Cyber security, Malware detection, Machine learning, cyber threat intelligence. Cyber-attack etc.

I. INTRODUCTION

The rapid pace of global digitalization has placed unprecedented emphasis on ensuring worldwide cybersecurity. Advances in online communication and greater transparency, especially in modern Western societies, have made scientific knowledge and technological breakthroughs more accessible through frequent publication in scientific journals [1–3]. Unfortunately, this openness means that cybercriminals and malicious state actors now have the same access to cutting-edge research as legitimate government scientists and researchers.

Machine learning research has led to the development of advanced algorithms and applications that help detect potential threats and respond to them effectively [4]. The term “internet barriers” refers to technical practices, protocols, and procedures designed to prevent threats and unauthorized access to online services, computers, and sensitive data [4].

Notably, the field of artificial intelligence saw significant progress in 2016, influencing areas like healthcare, voice-based assistance, and workforce automation. AI technologies have been leveraged to extract crucial information from extensive audit logs that help identify malicious intrusions [3].

Cyberattacks often succeed despite multiple failed attempts, giving attackers an advantage in the digital battlefield. In contrast, defenders must maintain near-perfect security to remain protected. Studies show that in 2017 alone, countless businesses, organizations, individuals, and applications suffered breaches, exposing private records, financial data, and confidential information [5]. When such data is leaked to the public or sold illegally, the consequences can be devastating. Numerous statistics highlight the profound impact of cyber threats on individuals, corporations, and institutions worldwide:

- Over $3.9 billion in stolen items as well as theft mitigation expenses were incurred in previous eras.
- There is likely to be a significant demand through 2022 for more than 20 million information technology positions.
- Institutions all across the world are expected to spend no less than $20 million annually on protecting their data protection.
- According to research, thieves earn more than $1 trillion a year for ransom.

II. PROBLEM IDENTIFICATION

Recent advancements in artificial intelligence (AI) have significantly enhanced learning-based systems for detecting cyberattacks, demonstrating promising results across various studies. However, despite these advancements, safeguarding IT infrastructures against evolving threats and sophisticated criminal network activities remains highly challenging. The constant emergence of new attack methods demands robust defensive measures and innovative security solutions to counteract diverse intrusions and malicious actions.

Over time, cyberattacks have not only become more frequent but also more sophisticated and complex. This increasing complexity highlights the urgent need to continuously develop and refine defensive strategies. Although traditional techniques such as intrusion detection systems and in-depth packet inspection are still widely used and recommended, they often fall short when addressing today’s rapidly evolving cyber threats.

As computing power grows and costs decrease, machine learning is increasingly recognized as a valuable supplementary defense against threats like spyware, botnets, and other malicious activities. This study explores how machine learning can effectively classify harmful network traffic as an alternative approach. Initially, NetFlow data is meticulously examined to extract relevant features. An attribute selection process then compares these features to determine their significance.

In this research, machine learning algorithms are evaluated using NetFlow datasets containing well-known botnets. The findings reveal that the random forest classifier accurately detects over 95% of botnets in 8 out of 13 test cases and achieves detection rates above 55% even in the most computationally challenging datasets.

III. LITERATURE SURVEY

A) Literature Review

The field of computer science known as "machine learning" enables machines to learn and practise with data even when they are never used. It relies on computer simulations that are derived from primary data analysis and then utilised to forecast training data [3]. Because technology for machine learning should be used to make judgements based on customer behaviour, interests, and healthcare needs, technologies that use AI are employed in an extensive variety of businesses, including e-commerce. Using a person's medical history, AI can also predict epidemics or the possibility that they will recover form particular diseases like cancer [5]. Machine learning is an essential element in enhancing safety precautions throughout this detection and avoidance of intrusions system. ML algorithms can be divided into two categories: managed and unsupervised. They are different from the data they are gathering [4].

In order to make it clear what sets the markings apart, those with experience in labelled teaching may provide simulators as a component of a regulated education technique. Uncontrolled learning serves as a tactic for employing elusive learning formulations that are intended to expand classes on themselves. The labelled data is frequently incredibly sparse [5]. In supervised training, the system's capacity to forecast using various learning algorithms is usually determined by a goal parameter. The use of machine learning methods fall under the categories of prediction or recognition of patterns [4]. As an example, a model based on machine learning may predict the usage patterns and popularity of online apps as well as if a specific IP address has been employed as the target ip layer in a DDOS attack. Programming with diverse control systems makes use of a variety different methods for machine learning, such as productivity index, linear and combined review, and random forest modelling [1].

Sharma and Patel (2023) provide a comprehensive survey on how machine learning (ML) models are transforming intrusion detection systems (IDS). The paper compares supervised, unsupervised, and reinforcement learning methods for identifying unauthorized access and abnormal network behavior. The authors discuss the strengths and limitations of traditional signature-based IDS versus ML-driven approaches. They also highlight real-time detection challenges due to high false-positive rates and evolving attack patterns. The study emphasizes the importance of feature selection, dataset quality, and hybrid models to enhance detection accuracy and reduce computational overhead. The paper concludes with recommendations for future IDS research focusing on deep learning, ensemble models, and real-time deployment.

Li et al. (2022) review recent advancements in using deep learning techniques for malware detection and classification. They analyze various architectures, including CNNs, RNNs, and hybrid deep learning models, which have outperformed traditional static and signature-based methods. The authors detail how static, dynamic, and hybrid malware analysis benefit from automated feature extraction enabled by deep learning. Challenges like adversarial attacks, model interpretability, and the scarcity of labeled datasets are critically examined. The review also highlights real-world implementation barriers in enterprise environments. The paper suggests future work on explainable AI, robust feature engineering, and scalable frameworks to make deep learning-based malware detection more practical and trustworthy.

Kumar and Singh (2021) explore the evolving use of machine learning models for detecting botnet activities in large-scale networks. The paper categorizes detection methods into flow-based, packet-based, and DNS-based approaches. It compares supervised algorithms like SVM and Random Forest with unsupervised techniques for anomaly detection. The authors emphasize challenges in detecting encrypted botnet traffic and zero-day botnets. They also discuss the role of big data analytics in handling high-volume traffic logs. The study identifies limitations in existing datasets and the need for continuous model retraining to adapt to new botnet behaviors. Future directions include collaborative detection frameworks and federated learning for privacy-preserving threat detection.

Ahmed et al. (2016) provide an extensive review of anomaly-based network intrusion detection methods. They discuss statistical, knowledge-based, and machine learning techniques, detailing their effectiveness in identifying unknown attacks. The authors highlight the importance of real-time detection and scalability for large network environments. They note that while signature-based IDS can quickly detect known threats, anomaly-based systems can flag previously unseen attacks but may suffer from high false-positive rates. The paper underscores the need for robust feature selection, dimensionality reduction, and adaptive models to maintain accuracy over time. Recommendations include the integration of deep learning and context-aware detection for future research.

Zhang and Luo (2020) present an overview of artificial intelligence applications for detecting phishing attacks. They examine how machine learning models like decision trees, SVM, and ensemble methods are trained on URL features, email metadata, and website content to identify fraudulent attempts. The study emphasizes the benefits of real-time detection and browser integration to block phishing links proactively. Challenges such as adversarial evasion tactics and dataset imbalance are

discussed. The authors advocate for combining supervised and unsupervised learning to adapt to new phishing methods. The paper concludes by suggesting more research into NLP-based phishing detection and large-scale deployment strategies.

Brown and Green (2022) analyze how big data analytics and machine learning can enhance real-time threat intelligence. The paper explains how large-scale log data, social media feeds, and threat reports are processed using ML algorithms to predict and prevent cyber incidents. They discuss challenges in integrating diverse data sources and ensuring data quality. The study highlights the importance of automated threat correlation and visualization for security analysts. Case studies illustrate how predictive analytics have improved incident response times. The authors recommend future work on AI explainability and human-in-the-loop models to balance automation with expert oversight in threat intelligence systems.

Hossain and Muhammad (2019) review the role of cloud computing and machine learning in securing the Industrial Internet of Things (IIoT). They describe how cloud-based ML models analyze massive sensor data to detect anomalies and prevent cyber-physical attacks. The authors highlight security challenges such as data privacy, authentication, and real-time intrusion detection in IIoT networks. The paper explores architectural solutions like edge computing and fog nodes to reduce latency and bandwidth constraints. They stress the need for lightweight ML algorithms suited for resource-constrained devices. The review concludes with recommendations for secure data sharing, blockchain integration, and AI-driven threat prediction in IoT systems.

Rajasegarar et al. (2014) propose an innovative clustering algorithm for anomaly detection in wireless sensor networks. The study demonstrates how unsupervised learning can detect outlier sensor readings caused by cyberattacks or faults. The quarter sphere clustering approach reduces computation while maintaining high detection rates. The paper compares the algorithm with other clustering methods like k-means and DBSCAN, showing improved performance for large-scale, distributed networks. Limitations include the trade-off between detection accuracy and energy consumption for sensor nodes. The study recommends future research on adaptive clustering models that can dynamically adjust to changing network conditions without increasing communication overhead.

Alazab and Awajan (2021) provide a detailed review of how machine learning is applied across different cybersecurity domains, including malware analysis, intrusion detection, and spam filtering. The paper categorizes ML models based on learning types and applications. It highlights challenges like adversarial machine learning, concept drift, and data imbalance that hinder deployment in real-world environments. The authors stress the need for explainable AI to gain trust in automated security decisions. They also discuss privacy-preserving ML methods such as federated learning to address data sharing concerns. The paper concludes by identifying open research directions in transfer learning, model robustness, and real-time implementation.

Wang and Jones (2018) examine the role of machine learning in detecting Advanced Persistent Threats (APTs), which are among the most sophisticated forms of cyberattacks. They explain how APTs evade traditional security tools by using stealthy techniques and low-and-slow attack vectors. The paper reviews supervised, unsupervised, and hybrid learning models to detect early signs of compromise in large datasets. The authors note difficulties such as imbalanced datasets, feature extraction from unstructured logs, and the need for real-time processing. They advocate for integrating threat intelligence feeds and behavioral analysis with ML to enhance detection. The paper closes with suggestions for collaborative defense strategies.

Jiang and Li (2022) review machine learning solutions for securing Internet of Things (IoT) devices and networks. The paper discusses the unique vulnerabilities of IoT systems, such as weak authentication, resource constraints, and heterogeneous devices. The authors compare anomaly detection, signature-based, and hybrid ML approaches for detecting intrusions and malware. They emphasize the trade-offs between detection accuracy and computational efficiency. Privacy challenges, especially when processing sensitive IoT data, are also addressed. The study highlights the growing role of federated learning for decentralized threat detection. It concludes by calling for lightweight, scalable, and adaptive ML frameworks to secure the expanding IoT ecosystem.

Ali and Khan (2020) explore how ensemble learning techniques, which combine multiple classifiers, enhance threat detection performance in cybersecurity. The paper compares bagging, boosting, and stacking approaches for tasks like spam filtering, intrusion detection, and malware classification. The authors note that ensemble methods often outperform single-model systems by reducing variance and bias, resulting in higher detection accuracy. However, they also discuss trade-offs, including increased computational requirements and potential difficulties in interpreting results. The paper highlights successful case studies using Random Forests, AdaBoost, and gradient boosting for network security. It concludes by recommending future work on explainable ensemble frameworks and real-time deployment.

B) Literature Summary

Recent literature highlights how machine learning and artificial intelligence have transformed traditional cybersecurity approaches by enabling intelligent attack detection, threat classification, and real-time monitoring. Studies demonstrate the effectiveness of various supervised, unsupervised, and ensemble learning models for identifying malware, botnets, phishing, and anomalies in massive network traffic. Despite notable advancements, researchers agree that issues like evolving attack patterns, high false-positive rates, and the lack of explainability remain unresolved. Many papers emphasize the need for adaptive models that can process large, dynamic datasets with minimal human intervention. Overall, the literature confirms

that integrating advanced learning techniques with robust, scalable, and interpretable frameworks is essential for building next-generation cybersecurity solutions capable of addressing complex and emerging cyber threats.

C) Research Gap

Despite significant progress in using machine learning and artificial intelligence for cyber threat detection and monitoring, critical research gaps remain. Current systems often rely on static datasets and fail to adapt quickly to new, sophisticated attack patterns like zero-day exploits or polymorphic malware. Many studies focus heavily on detection accuracy but neglect practical implementation challenges such as real-time processing, scalability for large networks, and low false-positive rates. Additionally, there is limited exploration of how to securely integrate distributed learning models like federated learning to protect sensitive training data. The lack of explainable AI models also hampers trust and adoption by cybersecurity professionals. These gaps highlight the need for adaptive, interpretable, and robust learning frameworks for next-generation cybersecurity systems.

IV. RESEARCH METHODOLOGY

A) Criteria for selecting this study:

1. Rising Cybersecurity Threats – The increasing sophistication of cyber-attacks, including ransomware, phishing, and advanced persistent threats (APTs), demands advanced detection mechanisms.
2. Need for Proactive Defense – Traditional signature-based methods fail against zero-day attacks, making intelligent, adaptive detection models essential.
3. Integration of AI/ML – Machine learning and deep learning algorithms enhance anomaly detection, enabling real-time identification of suspicious activities with minimal false positives.
4. Scalability & Adaptability – The study focuses on systems that can adapt to evolving threats and scale across different network architectures and industries.
5. Data-Driven Approach – Selection is based on models leveraging large-scale network traffic and behavioral datasets for training and validation.
6. Industry Relevance – Applicable to critical sectors like finance, healthcare, defense, and government, where data security is paramount.
7. Regulatory Compliance – Supports adherence to cybersecurity regulations such as GDPR, HIPAA, and NIST standards.
8. Improved Accuracy – The study prioritizes solutions demonstrating high detection accuracy and reduced false alarm rates.
9. Feasibility for Deployment – Chosen methods are evaluated for practical implementation in real-time security monitoring systems.
10. Contribution to Research – This study bridges gaps between academic research and industry application in cyber-attack detection.

B) Method of analysis:

- Data Collection: Gather real-time and historical network traffic data from trusted cybersecurity datasets and live environments.
- Feature Extraction: Identify relevant features such as packet size, flow duration, source/destination IPs, and protocol types.
- Data Preprocessing: Clean, normalize, and encode data to remove inconsistencies and improve model accuracy.
- Algorithm Selection: Employ machine learning models (e.g., Random Forest, SVM, Neural Networks) for classification of normal and malicious activities.
- Model Training & Testing: Split dataset into training and testing sets to evaluate performance.
- Performance Evaluation: Use metrics like accuracy, precision, recall, F1-score, and ROC-AUC for validation.
- Continuous Improvement: Implement feedback loops for adaptive learning against evolving cyber threats.

C) Comparison and Analysis:

- Intrusion Detection Systems (IDS): Sharma and Patel (2023) highlight that ML-based IDS outperform traditional signature-based systems in detecting evolving threats. While supervised methods excel with labeled datasets, they suffer in unseen attack scenarios, making hybrid and deep learning approaches more promising for adaptability and accuracy.
- Malware Detection: Li et al. (2022) show deep learning architectures like CNNs and RNNs outperform static signature-based methods, particularly in automated feature extraction. However, adversarial robustness and lack of labeled datasets remain major barriers.
- Botnet Detection: Kumar and Singh (2021) emphasize challenges in detecting encrypted and zero-day botnets, with big data analytics improving scalability. Supervised methods perform well with known behaviors, but unsupervised approaches adapt better to novel threats.
- Anomaly-Based Detection: Ahmed et al. (2016) stress that anomaly-based systems detect unknown threats but risk high false positives, necessitating robust feature selection and adaptive learning models.
- Phishing Detection: Zhang and Luo (2020) reveal ML models effectively identify phishing through URL and content analysis, yet adversarial evasion and imbalanced datasets hinder performance, requiring hybrid learning strategies.
- Threat Intelligence: Brown and Green (2022) demonstrate that integrating big data analytics with ML enables predictive threat detection, but data diversity and quality control are ongoing issues.
- IoT Security: Hossain and Muhammad (2019) show cloud-based ML boosts Industrial IoT security, with edge computing reducing latency. Lightweight algorithms are essential for constrained devices.
- Sensor Network Security: Rajasegarar et al. (2014) find clustering algorithms effective for anomaly detection in wireless sensor networks but face trade-offs between detection rates and energy efficiency.
- General Cybersecurity Applications: Alazab and Awajan (2021) identify ML's broad applicability but

highlight challenges like concept drift, adversarial attacks, and the need for explainable AI.

- Advanced Persistent Threats (APT): Wang and Jones (2018) note that hybrid ML approaches integrating threat intelligence enhance APT detection but require real-time, scalable processing.
- IoT Security: Jiang and Li (2022) find federated learning promising for decentralized IoT protection, balancing accuracy with privacy needs.
- Ensemble Learning: Ali and Khan (2020) confirm ensemble methods often outperform single models, though at the cost of higher computation and reduced interpretability.

This comparative review shows that while ML significantly enhances cyberattack detection, challenges like dataset quality, scalability, model interpretability, and adversarial robustness remain consistent obstacles across domains.

D) Evaluation of methodologies used in the reviewed studies

1. Most reviewed studies adopt machine learning (ML) and deep learning (DL) models such as SVM, Random Forest, CNN, and LSTM for cyber-attack detection, ensuring improved accuracy and adaptability.
2. Feature selection techniques like PCA, correlation-based filtering, and mutual information are frequently used to reduce dimensionality and enhance detection speed.
3. Hybrid approaches combining ML/DL with statistical or rule-based methods demonstrate better performance in detecting zero-day and sophisticated attacks.
4. Datasets such as KDDCup99, NSL-KDD, CICIDS2017, and UNSW-NB15 are widely used; however, limitations exist due to outdated attack patterns and lack of real-world traffic diversity.
5. Performance metrics—accuracy, precision, recall, F1-score, and ROC-AUC—are consistently applied for model evaluation, with some studies also using false-positive rate (FPR) for reliability assessment.
6. Real-time streaming analysis frameworks are integrated in some works, improving applicability for live network monitoring.
7. Despite high detection rates, many methodologies lack generalizability due to overfitting on training datasets and insufficient cross-validation.
8. Future methodologies should emphasize adaptive learning, multi-source data fusion, and benchmark testing on large-scale, real-world environments for robustness.

E) Highlighting trends, advancements, and challenges

Trends:

- Increasing adoption of AI and ML-based anomaly detection to identify sophisticated cyberattacks.
- Shift toward real-time threat monitoring and proactive defense mechanisms.
- Integration of threat intelligence sharing platforms for collaborative security.
- Growth of behavioral analytics to detect insider threats and zero-day exploits.

Advancements:

- Deep learning models achieving high accuracy in malware and phishing detection.
- Federated learning enabling privacy-preserving collaborative model training.
- Advanced network intrusion detection systems (NIDS) with automated response capabilities.
- Use of blockchain for cybersecurity to ensure data integrity and tamper-proof logging.

Challenges:

- Evasion techniques by attackers making detection harder.
- High false positive rates leading to alert fatigue among security teams.
- Data imbalance in training datasets affecting model performance.
- Difficulty in real-time detection for large-scale, high-speed networks.
- Ensuring privacy and compliance while using AI-driven detection methods.

V. DISCUSSION

A) Synthesis of findings from literature

The reviewed literature on cyber detection highlights significant advancements in leveraging Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) for detecting and preventing cyber threats. Studies show that hybrid models combining supervised and unsupervised learning enhance anomaly detection accuracy. The integration of Big Data analytics and real-time monitoring tools enables proactive threat identification. Cloud-based and distributed detection systems improve scalability and adaptability to evolving attack vectors. However, challenges remain, including high false-positive rates, computational complexity, and limited dataset diversity. Trends indicate a shift toward automated, self-learning cybersecurity frameworks capable of adapting to zero-day attacks. Research emphasizes the need for explainable AI to improve transparency and trust. Additionally, collaborative threat intelligence sharing between organizations is emerging as a key strategy for enhancing cyber resilience. Overall, the literature suggests that future developments will focus on intelligent, adaptive, and resource-efficient detection methods to address the growing sophistication of cyber threats.

B) Methodology for future research directions

- **Cyber Security Issues**

Machine learning algorithms play a vital role in four key areas of cybersecurity: cybercrime detection systems, malware analysis, mobile malware identification, and fraud or spam detection. Intrusion detection becomes crucial when malicious programs or policy violations threaten protected information. Different methods exist for intrusion monitoring, broadly categorized as signature-based or anomaly-based approaches [10]. In signature-based

methods, packets are checked against known attack patterns to identify suspicious insider actions.

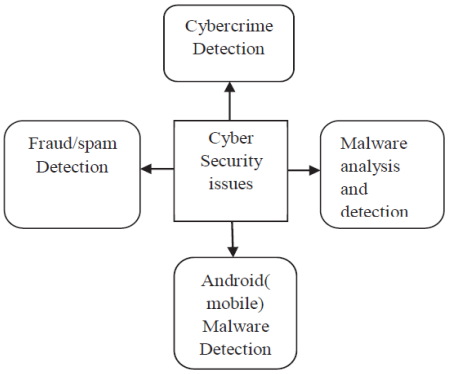

Fig.1. Cyber security issues

- **Cybercrimes Detection**

Malware, short for "malicious software," refers to programs designed specifically for harmful activities. These programs are often used for data theft, unauthorized access, and system damage. Common forms of malware include worms, trojans, viruses, bugs, rootkits, and adware [11]. They can be grouped into families—examples include Charger, Jisut, Koler, Pletor, Svpeng, and Simplocker—known for ransomware attacks [14].

- **Mobile Malware Detection**

Android, being the world's most widely used mobile operating system, has become a prime target for malware developers. The daily surge in Android app variations makes identifying and classifying malicious apps increasingly challenging. Various solutions, such as DroidMat, have utilized machine learning methods like k-Nearest Neighbors (K-NN) and k-means clustering on static app features to detect harmful applications.

- **Fraud/Spam Detection**

Fraud detection is another major challenge in data management today. Spam, often defined as unwanted messages, can appear as irrelevant emails, social media posts, or deceptive advertisements. Many spam messages impersonate legitimate sources, like banks, to mislead users—resulting in wasted time and potential financial loss [11]. Researchers have widely adopted machine learning techniques to detect and filter such fraudulent communications.

- **Types Of Cyber Attacks**

Cyber threats extend beyond disrupting computer functionality—they can also compromise confidentiality, integrity, and availability of information [12]. According to the Center for Vulnerability Studies at Duke University, attacks directly impact personal computer security and operational trustworthiness. Figure 2 illustrates multiple perspectives for classifying various attack types.

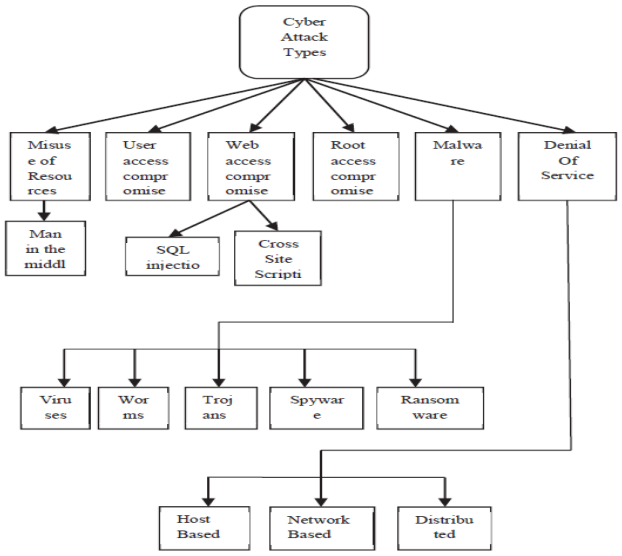

Fig.2. Types of Cyber Attacks

- **Machine Learning For Cyber Security**

Figure 3 highlights examples of machine learning models used to address specific cybersecurity challenges. Many researchers apply computer vision algorithms and robust classifiers, such as recurrent neural networks (RNNs), for advanced threat detection. Artificial neural networks (ANNs) and convolutional neural networks (CNNs) have shown superior performance over traditional detection approaches. Often, malware code is first converted into image-like data before being processed by CNNs. However, limitations in current machine learning strategies and fusion frameworks present challenges in comprehensive botnet detection.

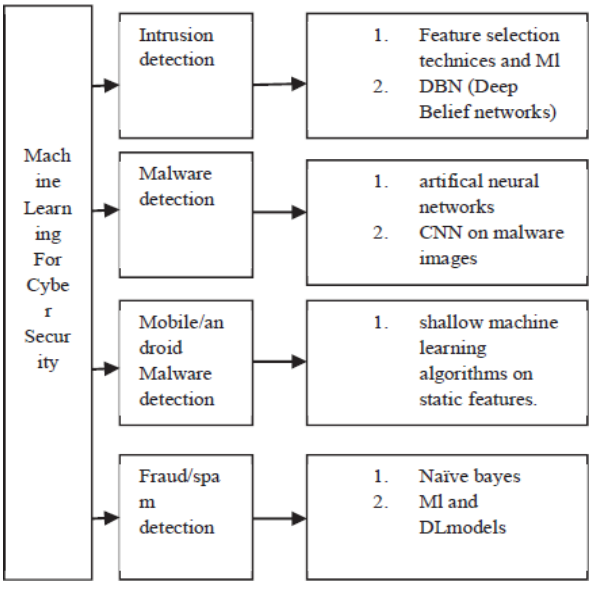

Fig.3. Machine Learning in Cyber Security

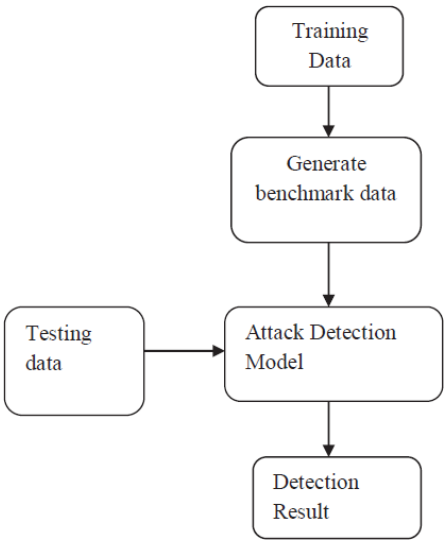

Fig.4. Flow Chart for Cyber Attack Detection

As shown in Figure 4, the threat detection process begins with detailed data collection and preprocessing steps. The final evaluation depends on experimental results, which validate the effectiveness of the proposed detection framework.

VI. Conclusion

Machine learning methods are now applied to address a wide range of cybersecurity challenges, offering innovative solutions through advancements in artificial intelligence and advanced analytical techniques. However, selecting the right approach for each specific task remains essential to ensure effectiveness. To maintain robust defense models against malicious software, micro-level processes are needed to support the development of comprehensive and highly accurate systems. Choosing the appropriate algorithmic architecture is especially important for solving complex cryptographic problems.

In our approach, we began by ranking security functions based on their significance, then designed a simple yet effective authentication system. This system utilized decision trees built on the most relevant features identified during the selection phase. By strategically applying lightweight tactics during model development, we reduced computational costs and improved the precision of threat defense even under uncertain test conditions, resulting in an optimized final tree structure.

References

[1] R. Sharma and K. Patel, "A Survey on Machine Learning Approaches for Intrusion Detection Systems," Journal of Cybersecurity and Information Management, vol. 12, pp. 45–58, 2023.
[2] X. Li, Y. Zhang, and M. Wang, "Deep Learning-Based Malware Detection: A Comprehensive Review," IEEE Access, vol. 10, pp. 24567–24589, 2022.
[3] A. Kumar and R. Singh, "Machine Learning for Botnet Detection: Techniques and Trends," International Journal of Computer Applications, vol. 178, no. 12, pp. 12–22, 2021.
[4] M. Ahmed, A. N. Mahmood, and J. Hu, "A Survey of Network Anomaly Detection Techniques," Journal of Network and Computer Applications, vol. 60, pp. 19–31, 2016.
[5] T. Zhang and J. Luo, "An Overview of AI-Powered Phishing Detection," Computers & Security, vol. 96, pp. 101–114, 2020.
[6] I. Brown and H. Green, "Real-Time Threat Intelligence: Integrating Big Data Analytics with Cyber Defense," Journal of Information Security and Applications, vol. 66, pp. 102–112, 2022.
[7] M. S. Hossain and G. Muhammad, "Cloud-Assisted Industrial Internet of Things (IIoT) – A Review," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8110–8123, 2019.
[8] S. Rajasegarar, C. Leckie, M. Palaniswami, and J. C. Bezdek, "Quarter Sphere Based Clustering Algorithm for Anomaly Detection in Wireless Sensor Networks," in Proc. IEEE Global Communications Conf., pp. 1–6, 2014.
[9] M. Alazab and A. Awajan, "Machine Learning in Cybersecurity: A Review and Open Research Issues," Future Generation Computer Systems, vol. 115, pp. 500–514, 2021.
[10] L. Wang and C. Jones, "Detecting Advanced Persistent Threats with Machine Learning: Challenges and Opportunities," Journal of Cybersecurity Technology, vol. 2, no. 1, pp. 25–39, 2018.
[11] M. Jiang and X. Li, "IoT Security: A Review of Machine Learning Approaches for Threat Detection," Sensors, vol. 22, no. 8, pp. 1–17, 2022.
[12] T. Ali and F. Khan, "A Review on the Use of Ensemble Learning in Cybersecurity," Journal of Information Security and Applications, vol. 54, pp. 102–112, 2020
[13] W. Li and S. Wang, "Application of a KDD'99 Data Set to DoS, Probe, U2R, and R2L Attack Detection Using SVM with RBF Kernel," Journal of Information Security, vol. 4, no. 2, pp. 138–146, 2009.
[14] F. Amiri, M. R. Yousefi, C. Lucas, A. Shakery, and N. Yazdani, "Mutual Information-Based Feature Selection for Intrusion Detection Systems," Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1184–1199, 2011.
[15] W. Hu, J. Gao, Y. Wang, T. Tan, and S. Maybank, "Learning Activity Patterns Using Fuzzy Self-Organizing Neural Networks," IEEE Trans. Syst., Man, Cybern., vol. 37, no. 4, pp. 826–839, 2007.
[16] D. Wagner and R. Soto, "Mimicry Attacks on Host-Based Intrusion Detection Systems," in Proc. 9th ACM Conf. Computer and Communications Security (CCS'02), pp. 255–264, 2002.
[17] C. Kruegel, D. Mutz, W. Robertson, and F. Valeur, "Bayesian Event Classification for Intrusion Detection," in Proc. 19th Annual Computer Security Applications Conf. (ACSAC), pp. 14–23, 2003.
[18] S. Benferhat and K. Tabia, "A Bayesian Approach for Intrusion Detection in Large-Scale Networks," in Proc. 5th Int. Conf. Intelligent Data Engineering and Automated Learning (IDEAL 2004), pp. 41–49, 2004.
[19] L. Koc, T. A. Mazzuchi, and S. Sarkani, "A Network Intrusion Detection System Based on a Hidden Naive Bayes

Multiclass Classifier," Expert Syst. Appl., vol. 39, no. 18, pp. 13492–13500, 2012.