Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Exploring the Applications of Machine Learning in Achieving Cyber Security

Dr Som Gupta
AKTU Lucknow

Abstract: - Cybersecurity has become a very challenging and an important aspect to be dealt with as almost everyone has access to the internet, and a computing device like Computers, Mobile Phones, Tablets, etc. Right from internet banking to commerce to entertainment to food services, almost every domain of life has been transformed because of the emergence of the internet.
Automatic ways to predict the probability of cyber crime to happen, can help prevent the cybercrime and thus ensure the safe usage of the internet and other services. The emergence of Artificial intelligence and machine learning techniques have improved the chances of predicting the complicated threats on time.
This paper discusses the use of Machine Learning and Deep Learning technologies to achieve cybersecurity in terms of detection of network intrusion, analysis of ransomware, malware detection, malicious file detection, system anomalies, security analysis, threat detections, unveiling phishing attacks, digital forensics, etc.
The paper also discusses the challenges in implementing machine learning techniques for efficient implementation of use cases for cybersecurity. The paper discusses the datasets available and the future scope implementing artificial intelligence based techniques for increasing cyber security.

Keywords: Malware;IDS;Cyber attacks;Machine Learning; Cybersecurity;

INTRODUCTION

The rapid proliferation of computing devices, the widespread adoption of the internet, and the exponential growth of online services have significantly increased concerns regarding cybersecurity. According to the World Bank, as of early 2025, approximately 66% of the global population uses the internet. The internet is extensively used for social networking, information retrieval, entertainment, e-commerce, travel, and health and wellness services. In parallel, the emergence of the Internet of Things (IoT) and mobile devices has led to a massive increase in the volume of digital data.

With the advent of 5G mobile communications, online activities are expected to further expand, highlighting the urgent need for robust cybersecurity infrastructures. The internet has increasingly become a target for cybercriminals, with the frequency and sophistication of attacks rising daily. Traditional methods of manually analyzing large volumes of network logs are inadequate, as attackers exploit system vulnerabilities through techniques such as phishing, pharming, vishing, and smishing. The growing sophistication of cyber threats underscores the need for automated and intelligent mechanisms to detect and prevent attacks [2].

Cybersecurity can broadly be classified into two primary domains: **infrastructure security** and **network security** [3].

Infrastructure security is concerned with protecting an organization's critical digital and physical assets. This includes safeguarding servers, databases, endpoints, data centers, cloud resources, and other IT infrastructure components from unauthorized access, data breaches, and operational disruptions. Effective infrastructure security involves implementing access controls, encryption mechanisms, identity management, patch management, and endpoint security solutions. Additionally, it encompasses the protection of operational continuity, ensuring that essential services remain functional during cyber attacks or system failures. Examples of infrastructure security measures include intrusion prevention systems (IPS), advanced firewalls, secure backup strategies, and anomaly detection tools that monitor system logs for unusual activities. With the proliferation of IoT devices and the increasing complexity of modern IT environments, infrastructure security has become a critical aspect of organizational resilience, as even minor vulnerabilities can have cascading effects on business operations.

Network security, in contrast, focuses on protecting data while it is transmitted across networks, ensuring its confidentiality, integrity, and availability. This domain addresses threats such as eavesdropping, man-in-the-middle attacks, packet sniffing, denial of service (DoS) attacks, and unauthorized network access. Network security involves techniques such as network segmentation, virtual private networks (VPNs), intrusion detection systems (IDS), intrusion prevention systems (IPS), secure routing protocols,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

encryption of data in transit, and monitoring of network traffic for anomalies. It also requires continuous adaptation to emerging threats, as attackers increasingly exploit vulnerabilities in network protocols, IoT connectivity, and wireless communications. Network security is particularly critical in enterprise environments where large volumes of sensitive data, including personal information, financial records, and intellectual property, are transmitted across interconnected systems.

Together, **infrastructure and network security provide a comprehensive defense strategy**, ensuring that both the foundational IT assets and the data flowing across them are protected. While infrastructure security safeguards the "static" components of an organization's digital ecosystem, network security protects the "dynamic" data interactions, and a failure in either domain can compromise the overall cybersecurity posture. With the rise of cloud computing, edge devices, and 5G connectivity, the interplay between infrastructure and network security has become increasingly complex, demanding integrated approaches that combine monitoring, threat detection, and automated response mechanisms.

The increasing volume of network logs, shortage of skilled cybersecurity professionals, and vulnerabilities in system configurations have amplified the risk of cyber attacks. In response, automated techniques such as Machine Learning (ML) and Deep Learning (DL) have emerged as efficient tools for detecting and preventing cyber threats. Supervised ML techniques, for example, analyze file attributes to classify them as benign or malicious, enabling proactive threat mitigation. A review of approximately 100 research studies from leading databases indicates that the application of machine learning in cybersecurity is still in its early stages.

Machine learning has already been successfully applied across diverse domains such as finance, medicine, education, and manufacturing. Its integration into cybersecurity aims to create intelligent systems capable of making autonomous decisions. By training models on historical data, these techniques can predict and respond to new threats in real time. Commonly used models in cybersecurity include **Random Forests, Support Vector Machines (SVM), Logistic Regression, K-Nearest Neighbors (KNN), Decision Trees, and Convolutional Neural Networks (CNNs)**. While traditional security mechanisms such as firewalls, antivirus software, and intrusion prevention systems remain important, studies indicate that machine learning-based approaches often provide superior performance in detecting complex and evolving cyber threats [4][8].

Few of the use cases of using ML for CyberSecurity are:
Fraud Detection
Network Intrusion Detection
Spam Identification
Malware Identification
Detection of System Anomalies
Predictive Risk Scoring

RELATED WORKS

The field of cybersecurity has witnessed extensive research over the past decades, with machine learning and AI increasingly integrated to enhance threat detection, mitigation, and response. Several studies have contributed to taxonomies, predictive models, and framework-based analyses of cyber threats.

Kotapati et al. [5] (2005) proposed a taxonomy for cyber attacks on mobile devices, classifying them into three categories:

- **Physical attacks**: unauthorized access to the physical device,
- **Attack types**: interception, fabrication, modification, denial of service (DoS), and interruption,
- **Attack means**: messages, data, and service logic.

This taxonomy is largely applicable to other computing devices and provides a structured framework to understand different attack vectors.

Similarly, Mohamed et al. (2015) provided a broader taxonomy for cybersecurity research, dividing it into Intrusion Detection, Behavioral Analysis, Threat Intelligence, Automated Response, and Malware Classification. Their analysis revealed that most research efforts have focused on Intrusion Detection and Malware Classification. The evolution of cybersecurity threats over time has been observed as follows: early Internet usage was dominated by denial of service attacks, followed by phishing attacks during

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

the rise of e-commerce. The proliferation of botnets and malware emerged with increased antivirus adoption. By the late 2010s, AI and machine learning became prominent tools for addressing cybersecurity challenges.

Duary et al. [11] (2024) explored predictive analytics for detecting cyber threats, emphasizing the importance of proactive threat identification using historical and real-time data.

Chan et al. [12] (2025) employed supervised learning techniques to detect cyber threats, demonstrating the effectiveness of classification-based approaches for threat detection in dynamic network environments.

Ramapreet et al. [13] highlighted the application of the **NIST Cybersecurity Framework**, which consists of five key functions: Identification, Protection, Detection, Response, and Recovery.

- **Identification** involves assessing the current cybersecurity posture and detecting vulnerabilities. Techniques such as K-Means clustering and Random Forests are widely used to identify vulnerable devices based on traffic conditions and network configurations.
- **Risk Assessment** entails evaluating potential threats and prioritizing mitigation strategies. Deep learning, source code analysis, and transfer learning have been utilized to identify and quantify risks.
- **Protection** encompasses AI-driven security mechanisms, including user and device authentication, automatic access control, domain blocking, and dynamic backup scheduling.

Several studies have explored ML-based techniques for threat classification and vulnerability analysis:

- Meyers et al. [14] applied word embeddings and agglomerative clustering in NLP to group vulnerabilities and identify relationships between them.
- Maimo et al. [15] integrated machine learning with Network Function Virtualization (NFV) and Software Defined Networking (SDN) to classify ransomware and detect network anomalies.
- Sakhinini et al. [16] used ensemble machine learning methods for intrusion detection in physical layer security.
- Garcia et al. [17] predicted the severity of cybersecurity events using various ML algorithms, including AdaBoost, Gradient Boosting, Random Forests, Decision Trees, Multilayer Perceptron, and K-Means clustering. Their work demonstrated the potential of ML for proactive risk management and prioritization of security incidents.

DATASETS AVAILABLE FOR MACHINE LEARNING IN CYBERSECURITY

A variety of benchmark datasets are available to support research in applying machine learning techniques to cybersecurity problems such as intrusion detection, malware classification, and network anomaly detection. Some of the most widely used datasets are described below:

1. KDD Cup 1999 Dataset

The KDD Cup 1999 dataset was originally developed for the KDD competition on data mining and intrusion detection. It is one of the earliest and most extensively used datasets in cybersecurity research. The dataset contains approximately 4 million instances of network traffic records, labeled as either normal or malicious. It is primarily used to evaluate machine learning algorithms for detecting intrusive activities in network communications.

2. NSL-KDD Dataset

The NSL-KDD dataset is an improved version of the KDD Cup 1999 dataset. It addresses key issues such as redundancy and imbalance present in the original dataset. By removing duplicate records and providing a more balanced distribution, NSL-KDD enables more reliable evaluation of machine learning models.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

3. EMBER Dataset

The EMBER (Endgame Malware Benchmark for Research) dataset was introduced by Anderson et al. for developing static malware detection models. It focuses on the classification of malicious Windows Portable Executable (PE) files. The dataset contains approximately 1.1 million samples, including around 900,000 training instances and 200,000 testing instances, along with extracted features suitable for machine learning tasks.

4. PCAP Files

Packet Capture (PCAP) files are widely used in network traffic analysis. They contain detailed packet-level information such as source and destination IP addresses, port numbers, protocol types, and Time-to-Live (TTL) values. Researchers use PCAP data to study network behavior, detect anomalies, and identify potential cyber threats in real-world traffic.

5. Kaggle Datasets

Kaggle hosts a wide range of publicly available datasets relevant to cybersecurity. These datasets cover various attack scenarios, including phishing, malware detection, and network intrusion. Kaggle also provides a collaborative environment for benchmarking machine learning models and sharing experimental results.

6. DARPA Dataset

The DARPA intrusion detection dataset is another foundational resource in cybersecurity research. It includes network traffic data capturing communication between source and destination IP addresses. Additionally, it provides diverse data types such as network sniffing data, Basic Security Module (BSM) audit logs, NT audit logs, and directory structure information. This dataset is commonly used for evaluating intrusion detection systems.

Table1: Comparative Study of the mentioned datasets

Dataset	Data Type	Size / Scale	Application Area	Strengths	Limitations
KDD Cup 1999	Network traffic features	~4 million instances	Intrusion Detection	Large dataset, widely benchmarked	High redundancy, outdated attack patterns
NSL-KDD	Network traffic features	Reduced subset of KDD	Intrusion Detection	Less redundancy, balanced dataset	Still lacks modern attack scenarios
EMBER	Static PE file features	~1.1 million samples	Malware Detection	Realistic, large-scale, feature-rich	Limited to Windows PE files, static analysis only
PCAP Files	Raw network packets	Variable (depends on capture)	Network Analysis, IDS	Highly detailed, real-world traffic representation	Large size, requires

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

					preprocessing, labeling challenges
Kaggle Datasets	Mixed (varies by dataset)	Varies (small to large datasets)	Multiple cybersecurity tasks	Diverse datasets, easy accessibility	Inconsistent quality, lack of standardization
DARPA	Network traffic + logs	Moderate (varied components)	Intrusion Detection	Multi-source data (logs + traffic), benchmark dataset	Synthetic environment, outdated scenarios

APPLICATIONS OF MACHINE LEARNING IN CYBERSECURITY

Machine learning (ML) techniques have been widely adopted in cybersecurity to detect, prevent, and mitigate various types of cyber threats. Key application areas are discussed below:

1. Phishing Detection

Phishing is a form of cybercrime in which malicious actors use deceptive URLs or emails to obtain sensitive user information such as login credentials and financial data. Detecting phishing websites is a challenging task due to their resemblance to legitimate sites.

Machine learning-based approaches enable automated phishing detection by leveraging features extracted from URLs, webpage structure, and email components such as headers, body text, and attachments. Additionally, information from blacklisted websites enhances detection accuracy. Various classification techniques, including Random Forest, Support Vector Machines (SVM), Logistic Regression, and Decision Trees, have been employed for this purpose. Peng et al. utilized blacklist-based features, while Sahingoz et al. categorized features into Natural Language Processing (NLP)-based, word vector-based, and hybrid features. Their study demonstrated that NLP-based features outperform word vector approaches. Similarly, Routhu et al. applied Random Forest algorithms using features derived from URLs, source code, and third-party services to improve phishing detection performance.

2. Anomaly Detection

Anomaly detection focuses on identifying unusual patterns in network traffic, system logs, and user behavior that deviate from normal activity. It plays a critical role in detecting previously unknown or zero-day attacks.

Machine learning models for anomaly detection include supervised, semi-supervised, unsupervised, and deep learning approaches. These models learn normal behavior patterns and flag deviations as potential threats. Commonly used techniques include Support Vector Machines (SVM), Neural Networks, Logistic Regression, and K-Nearest Neighbors (KNN). The effectiveness of anomaly detection lies in its ability to identify novel and evolving attack patterns without relying on predefined signatures.

3. Malware Detection

Malware detection involves identifying malicious software designed to disrupt systems, steal data, or gain unauthorized access. Common types of malware include viruses, Trojan horses, spyware, worms, adware, ransomware, rootkits, backdoors, and botnets.

Machine learning techniques analyze large volumes of system and network data to detect malicious patterns and adapt to emerging threats. Feature extraction is typically performed using:

- **Static analysis**: Examining code without execution

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

- **Dynamic analysis**: Monitoring runtime behavior such as API calls, network traffic, and registry changes

4. Network Intrusion Detection

Network Intrusion Detection Systems (NIDS) are designed to monitor and analyze network activities to identify unauthorized access or malicious behavior. These systems can be broadly classified into:

- **Network-based intrusion detection systems (NIDS)**
- **Host-based intrusion detection systems (HIDS)**

Machine learning enhances intrusion detection by analyzing diverse data sources such as full packet captures, network flow data, Domain Name System (DNS) records, and Simple Network Management Protocol (SNMP) data. These approaches improve detection accuracy and enable real-time threat identification.

5. SQL Injection Detection

SQL injection is a critical vulnerability in which malicious SQL queries are inserted into input fields to manipulate databases and gain unauthorized access.

Machine learning techniques can assist in detecting SQL injection attacks by analyzing query patterns and identifying deviations from normal query structures. Both static code analysis and dynamic runtime analysis are commonly used to detect such vulnerabilities. These approaches help in proactively securing web applications against database-level attacks.

6. Spam Detection

Spam detection involves identifying unsolicited and often malicious emails sent in bulk for advertising, phishing, or spreading malware. Spam emails consume network bandwidth, storage resources, and degrade user experience.

Machine learning-based spam filters classify emails as spam or legitimate based on features such as content, metadata, and sender behavior. Techniques such as Random Forests, Naïve Bayes, and Support Vector Machines have been widely used. For example, Lee et al. utilized feature-based approaches with Random Forest classifiers to effectively detect spam emails.

CHALLENGES IN APPLYING MACHINE LEARNING TO CYBERSECURITY

Despite the significant advancements in applying machine learning techniques to cybersecurity, several challenges remain that limit their effectiveness and real-world deployment. These challenges are discussed below:

1. Availability of High-Quality Datasets

The performance of machine learning models heavily depends on the quality and availability of datasets. However, cybersecurity is a relatively evolving research domain, and there is a lack of comprehensive, high-quality datasets with reliable labels.

Many existing datasets suffer from issues such as inconsistency, limited diversity of attack types, and outdated information. An ideal dataset should include raw network traffic, audit logs, and system-level data, along with properly labeled instances of both normal and malicious activities. Furthermore, datasets must be regularly updated to incorporate emerging and sophisticated attack patterns. Compliance with ethical standards and acceptance by the research community are also essential for ensuring reproducibility and fairness in model evaluation.

2. False Positives and False Negatives in Intrusion Detection Systems

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Machine learning-based Intrusion Detection Systems (IDS) often face challenges related to misclassification, particularly false positives and false negatives.

- **False positives** occur when benign activities are incorrectly classified as malicious, leading to unnecessary allocation of resources and potential disruption of normal operations.
- **False negatives**, on the other hand, occur when actual threats are not detected, which can result in severe security breaches and system compromise.

Balancing detection accuracy while minimizing these errors remains a critical challenge in the deployment of reliable cybersecurity systems.

3. Limited Access to Multiple Data Sources

Effective threat detection often requires the integration of data from multiple heterogeneous sources, such as network traffic, system logs, user behavior, and application-level data. However, many current machine learning approaches operate on isolated datasets and fail to leverage multi-source data effectively.

This limitation reduces the overall visibility of the system and may lead to incomplete or inaccurate threat detection. Integrating diverse data sources while maintaining scalability and efficiency remains an open research problem.

4. Transparency and Trustworthiness of AI Systems

The lack of transparency in machine learning models, particularly in complex models such as deep learning, poses a significant challenge in cybersecurity applications. These models often function as “black boxes,” making it difficult to interpret their decisions.

For cybersecurity systems, explainability and transparency are crucial for building trust among users and security professionals. The ability to understand why a model classified an activity as malicious or benign is essential for validation, debugging, and compliance with regulatory requirements. Therefore, developing explainable and trustworthy AI systems is a key research direction.

FUTURE AREAS OF RESEARCH

The rapid evolution of cybersecurity threats and the increasing reliance on machine learning (ML) techniques highlight several critical areas for future research:

1. Improving Intrusion Detection Systems

Current Intrusion Detection Systems (IDS) face challenges such as dataset imbalance and feature multi-collinearity, which can adversely affect model performance. Future research should focus on developing techniques to handle these issues, such as advanced sampling methods, feature selection, and dimensionality reduction. Additionally, emerging IDS research must incorporate fairness, bias mitigation, transparency, privacy, and security considerations to ensure that AI models are both effective and ethically compliant.

2. Advanced Threat Detection

Machine learning has shown potential in detecting complex cyber threats by analyzing network traffic, system behavior, and user activity. Future research should focus on detecting **zero-day exploits**, **polymorphic malware**, and other sophisticated attacks that do not follow known patterns. Developing ML models capable of recognizing previously unseen threats will significantly enhance organizational cyber defense capabilities.

3. Robust and Adaptive AI Models

Most existing AI models are trained on historical datasets, which limits their ability to detect novel and rapidly evolving cyber threats. As cybercriminals continuously develop new attack strategies, classifiers trained on outdated datasets may produce

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

inaccurate predictions. Future research should prioritize the development of **robust and adaptive AI models** that can generalize across a wide range of cyber threats and dynamically update their knowledge as new data becomes available.

4. Development of Benchmark Datasets

While numerous datasets exist for cybersecurity research, identifying datasets that meet benchmark standards remains challenging. There is a pressing need to create **high-quality, balanced, and representative datasets** that include diverse attack types, realistic network behaviors, and comprehensive labeling. Such datasets will support reproducible research, improve model evaluation, and accelerate the development of effective cybersecurity solutions.

CONCLUSION

In today's world, cybersecurity is a global concern. Machine Learning is a simple and economical way to prevent cyber attacks. The ability of Machine Learning to recognize the patterns and learn the hidden patterns has made it a popular way to detect the cyber threats as the emergence of IoT and the exponential increase of traffic and data has necessitated the need of automatic ways to prevent and detect the possible threats which can affect the infrastructure and lead to loss of finance and data. Nowadays a lot of research has been conducted to detect the spam emails, phishing emails, Intrusion detection, etc. Overall, machine learning provides scalable and adaptive solutions across multiple domains of cybersecurity. From phishing and spam detection to malware analysis and intrusion detection, ML-based systems significantly enhance the ability to detect both known and emerging threats. However, the effectiveness of these systems depends heavily on the quality of data, feature engineering, and the choice of algorithms. Challenges such as limited dataset availability, classification errors, lack of multi-source data integration, and insufficient model transparency continue to hinder the effectiveness of machine learning in cybersecurity. Addressing these issues is essential for developing robust, reliable, and scalable security solutions.The paper has listed most of the cyber security attacks and the works done in those areas using machine learning. The paper has discussed the works done in the particular areas, challenges, datasets available and the future directions for further research in this field. Future research in machine learning for cybersecurity must focus on improving IDS performance, detecting advanced threats, developing robust AI models, and creating high-quality benchmark datasets. Addressing these areas will strengthen the resilience and adaptability of AI-driven cybersecurity systems in the face of increasingly sophisticated cyber threats.

REFERENCES

[1] World Bank, "Internet users (% of population)," World Bank Open Data. [Online]. Available: https://data.worldbank.org/indicator/IT.NET.USER.ZS
[2] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A survey on machine learning techniques for cyber security in the last decade," IEEE Access, vol. 8, pp. 222310–222354, 2020, doi: 10.1109/ACCESS.2020.3041951.
[3] M. M. Inuwa and R. Das, "A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks," Internet of Things, vol. 26, p. 101162, 2024, doi: https://doi.org/10.1016/j.iot.2024.101162.
[4] R. S. Rao and A. R. Pais, "Detection of phishing websites using an efficient feature-based machine learning framework," Neural Comput. Appl., vol. 31, no. 8, pp. 3851–3873, Aug. 2019.
[5] K. Kotapati, P. Liu, Y. Sun, and T. F. LaPorta, "A taxonomy of cyber attacks on 3G networks," in Proc. Int. Conf. Intell. Secur. Inform., Berlin, Germany: Springer, 2005, pp. 631–633.
[6] B. Narwal, A. K. Mohapatra, and K. A. Usmani, "Towards a taxonomy of cyber threats against target applications," J. Statist. Manage. Syst., vol. 22, no. 2, pp. 301–325, Feb. 2019.
[7] H. Bahassi, N. Edddermoug, A. Mansour, and A. Mohamed, "Toward an exhaustive review on machine learning for cybersecurity," Procedia Comput. Sci., vol. 203, pp. 583–587, 2022, ISSN 1877-0509.
[8] Z. He, D. Davila, S. Bi, T. Wang, and T. Hou, "Machine learning for cybersecurity: A survey of applications, adversarial challenges, and future research directions," Electronics, vol. 14, no. 23, p. 4563, 2025, doi: https://doi.org/10.3390/electronics14234563.
[9] N. Mohamed, "Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms," Knowl. Inf. Syst., vol. 67, pp. 6969–7055, 2025, doi: https://doi.org/10.1007/s10115-025-02429-y.
[10] S. Samtani, H. Chen, M. Kantarcioglu, and B. Thuraisingham, "Explainable artificial intelligence for cyber threat intelligence (XAI-CTI)," IEEE Trans. Dependable Secure Comput., vol. 19, no. 4, pp. 2149–2150, 2022.
[11] S. Duary, P. Choudhury, S. Mishra, V. Sharma, D. D. Rao, and A. P. Aderemi, "Cybersecurity threats detection in intelligent networks using predictive analytics approaches," in Proc. 4th Int. Conf. Innovative Practices Technol. Manage. (ICIPTM), IEEE, 2024, pp. 1–5.
[12] L. Chan, I. Morgan, H. Simon, F. Alshabanat, D. Ober, J. Gentry, D. Min, and R. Cao, "Survey of AI in cybersecurity for information technology management," in Proc. 2019 IEEE Technol. Eng. Manage. Conf. (TEMSCON), 2019, pp. 1–8.
[13] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," Inf. Fusion, vol. 97, p. 101804, 2023, ISSN 1566-2535, doi: https://doi.org/10.1016/j.inffus.2023.101804.
[14] B. S. Meyers and A. Meneely, "An automated post-mortem analysis of vulnerability relationships using natural language word embeddings," Procedia Comput. Sci., vol. 184, pp. 953–958, 2021, ISSN 1877-0509.
[15] L. Fernandez Maimo, A. Huertas Celdran, A. L. Perales Gomez, F. J. Garcia Clemente, J. Weimer, and I. Lee, "Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments," Sensors, vol. 19, no. 5, p. 1114, 2019.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

[16] J. Sakhnini, H. Karimipour, A. Dehghantanha, and R. M. Parizi, "Physical layer attack identification and localization in cyber–physical grid: An ensemble deep learning based approach," Phys. Commun., vol. 47, 2021.
[17] N. DeCastro-García, A. L. Muñoz Castañeda, and M. Fernández-Rodríguez, "Machine learning for automatic assignment of the severity of cybersecurity events," Comput. Math. Methods Med., vol. 2, no. 1, 2020.
[18] H. S. Anderson and P. Roth, "EMBER: An open dataset for training static PE malware machine learning models," arXiv preprint arXiv:1804.04637v2, 2018.
[19] E. Berrueta, D. Morato, E. Magaña, and M. Izal, "Crypto-ransomware detection using machine learning models in file-sharing network scenario with encrypted traffic," Expert Syst. Appl., 2022. [Online]. Available: https://paperswithcode.com/paper/crypto-ransomware-detection-using-machine
[20] S. K. H. Ahammad, S. D. Kale, G. D. Upadhye, S. D. Pande, E. V. Babu, A. V. Dhumane, and D. K. J. Bahadur, "Phishing URL detection using machine learning methods," Adv. Eng. Softw., vol. 173, p. 103288, 2022, doi: https://doi.org/10.1016/j.advengsoft.2022.103288.
[21] N. Kshetri, "Economics of artificial intelligence in cybersecurity," IEEE IT Prof., vol. 23, no. 5, pp. 73–77, 2021.
[22] O. K. Sahingoz, E. Buber, O. Demir, and B. Diri, "Machine learning based phishing detection from URLs," Expert Syst. Appl., vol. 117, pp. 345–357, 2019, doi: https://doi.org/10.1016/j.eswa.2018.09.029.
[23] T. Peng, I. Harris, and Y. Sawa, "Detecting phishing attacks using natural language processing and machine learning," in Proc. 2018 IEEE 12th Int. Conf. Semantic Comput. (ICSC), 2018, doi: 10.1109/icsc.2018.00056.
[24] L. K. Kumari, K. Balasubramanian, K. Ramalakshmi, B. Mohan, R. S. Krishnan, and J. R. F. Raj, "Anomaly detection in cybersecurity using machine learning classifiers," in Proc. 2025 6th Int. Conf. Recent Advances Inf. Technol. (RAIT), Dhanbad, India, 2025, pp. 1–6, doi: 10.1109/RAIT65068.2025.11089051.
[25] S. A. Mohammed and S. Behadili, "Malware detection using machine learning techniques: A review," Basra J. Sci., vol. 42, 2025, doi: 10.29072/basjs.20240205.
[26] S. M. Lee, D. S. Kim, J. H. Kim, and J. S. Park, "Spam detection using feature selection and parameters optimization," in Proc. Int. Conf. Complex, Intell. Softw. Intensive Syst., Feb. 2010, pp. 883–888.