

A State of The Art Review of Machine Learning Approches for Cyber Security

¹Dr. A.Vinoth, ²Ms. M. Vijaya Sri

Assistant Professor, Department of Information Technology, Sri Krishna Adithya College of Arts and Science, Coimbatore, Tamil Nadu, India.

³rd Year Student, Department of Information Technology, Sri Krishna Adithya College of Arts and Science, Coimbatore, Tamil Nadu, India.

¹vino.asstprof@gmail.com, ²Vijayasrimarivel26@gmail.com

Abstract

Cybercrime is growing rapidly and takes advantage of weaknesses in today's computing systems. Ethical hackers play an important role in identifying these weaknesses and proposing effective methods to reduce security risks. As cyber threats continue to evolve, the cybersecurity community faces an urgent need for advanced and reliable protection techniques.

In recent years, machine learning has become increasingly important in cybersecurity because of its ability to analyze large amounts of data and identify complex attack patterns. Machine learning approaches are commonly applied to key security tasks such as intrusion detection, malware detection and classification, spam filtering, and phishing detection.

While machine learning alone cannot fully automate cybersecurity operations, it significantly improves the efficiency and accuracy of threat detection compared to traditional rule-based methods, thereby reducing the workload of security professionals.

The constantly changing nature of cyber threats presents ongoing challenges for researchers, requiring a strong combination of expertise in both cybersecurity and data science. This paper reviews recent machine learning-based cybersecurity solutions and examines the effectiveness of various algorithms in addressing common cyber threats.

Keywords: Cybersecurity, Malware detection, Machine learning, Deep learning.

1.INTRODUCTION:

Since the emergence of internet technology, cyberspace has become a major platform for cyber-attacks. Rapid technological advancements have enabled attackers to more easily identify system weaknesses and develop malicious software, including viruses and malware, which continuously challenge the cybersecurity industry. Cybersecurity focuses on creating a secure computing and communication environment through appropriate technologies, policies, and practices aimed at protecting computers, networks, applications, and data from attacks, unauthorized access, modification, or destruction.

Modern security infrastructures consist of both network-level and host-based protection mechanisms such as firewalls, antivirus software, and intrusion detection systems. Machine learning has demonstrated strong capabilities in addressing complex problems across various domains,

including image processing, healthcare informatics, computational biology, robotics, financial forecasting, audio and video analysis, and text processing [1].

In recent years, machine learning techniques have also been effectively applied to cybersecurity to design intelligent and adaptive defense solutions. Due to their ability to learn patterns from large volumes of data, machine learning models show great potential in identifying and predicting different types of cyber-attacks, making them a vital tool for security professionals. A survey conducted by ESET on the adoption of machine learning in cybersecurity reported that nearly 80% of respondents believe that machine learning enables faster threat detection and response within their organizations [9].

2. MACHINE LEARNING TECHNIQUES

2.1 Regression:

Regression is a supervised machine learning technique used to predict the value of a dependent variable based on one or more independent variables. The model learns from historical data and applies this learned knowledge to estimate outcomes for new or unseen data. In the context of cybersecurity, regression methods are commonly applied in areas such as fraud detection.

After training a model on past transaction data, the system can analyze the features of current transactions and identify potentially fraudulent activities. Various machine learning algorithms support regression analysis, including Linear Regression, Polynomial Regression, Support Vector Machines, Decision Trees, and Random Forests.

Venkatesh Jaganathan[2] et.al applied multiple regression methods to predict the impact of cyberattacks. In their work, the Overall CVSS (Common Vulnerability Scoring System) score was used as the dependent variable, while the number of vulnerabilities (X1) and average input network traffic (X2) were used as independent variables.

Similarly, Daria Lavrova [3] et al. proposed a multiple regression-based approach for detecting security incidents in Internet of Things (IoT) environments, which proved effective in identifying both known and unknown attacks.

2.2 Classification:

Classification is another widely used supervised learning approach in machine learning, where data instances are assigned to predefined categories or classes. In cybersecurity, classification techniques are extensively used for tasks such as spam detection, where email messages are categorized as spam or legitimate. Machine learning-based classifiers are capable of learning distinguishing features that separate malicious content from normal data. Common classification algorithms include Logistic Regression, k-Nearest Neighbors, Support Vector

Machines, Naïve Bayes, Decision Trees, and Random Forest classifiers. With the availability of large labeled datasets, deep learning-based classification models have become increasingly effective. These models often use architectures such as Restricted Boltzmann Machines (RBMs), Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks for automated feature extraction, followed by fully connected layers for classification. However, the performance of supervised classification methods largely depends on the availability and quality of labeled training data.

2.3 Clustering:

Unlike regression and classification, which require labeled data, clustering is an unsupervised learning technique that identifies inherent patterns in unlabeled datasets. In cybersecurity clustering is useful for discovering unknown threats and unusual behaviour. This helps security analysts detect new types of attacks that do not match existing signature. Clustering groups data instances into clusters based on similarity, where each cluster represents a distinct behavioral or structural pattern. In cybersecurity applications, clustering techniques are useful for tasks such as anomaly detection, forensic investigation, and malware analysis, as they help uncover previously unknown attack behaviors. Common clustering algorithms used in cybersecurity include K-means, K-medoids, DBSCAN, Gaussian Mixture Models, and Agglomerative clustering. In addition, neural network-based approaches such as Self-Organizing Maps (SOMs) are also employed to perform clustering by projecting high-dimensional data into lower-dimensional representations while preserving similarity relationships. Overall clustering helps cyber security systems adapt to evolving threats by identifying unknown attack patterns and reducing the dependency on labelled datasets.

3. CYBER SECURITY ISSUES:

The four major areas where Machine Learning algorithms play a crucial role are Intrusion Detection Systems, Malware analysis, Mobile (Android) malware detection and Spam Detection.

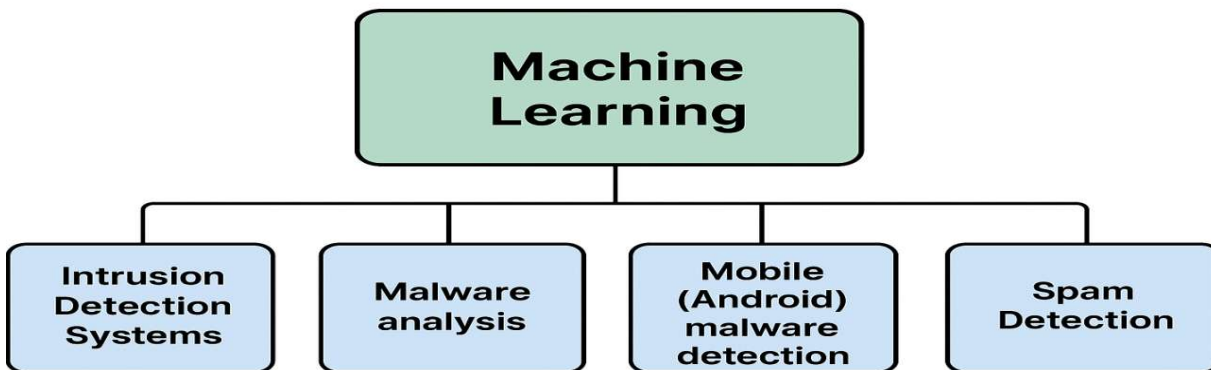


Figure 1: Cyber security issues

3.1. Intrusion Detection Systems:

Intrusion Detection Systems (IDS) are used when secure information is threatened due to malicious software activities or violations of security policies. These systems help in identifying unauthorized access or abnormal behavior within a network. Intrusion detection methods are generally divided into two main categories: signature-based detection and anomaly-based detection.

In signature-based detection, incoming network packets are examined and matched against a database of known attack patterns or signatures. If a match is found, the activity is identified as an intrusion. On the other hand, anomaly-based detection works by continuously monitoring network traffic and comparing it with a predefined model of normal behavior. Any significant deviation from this normal pattern is considered suspicious.

Saroj Kr. Biswas[4] demonstrated that machine learning-based feature selection techniques significantly improve the performance of intrusion detection systems. By combining multiple feature selection methods, their approach achieved better detection accuracy. R. Vinaya Kumar[5] et.al introduced a hybrid IDS model named AlertNet, which analyzes both network-level and host-level activities. This system was built using Deep Neural Networks (DNNs) and implemented on a scalable big data framework using Apache Spark. They evaluated their model

on widely used datasets such as CICIDS 2017, KDDCup 99, UNSW-NB15, NSL-KDD, and WSN-DS. The experiments were conducted with various learning rates ranging from 0.01 to 0.5 and trained over 1000 epochs. Traditional machine learning models were also used as baseline methods for comparison.

Md. Zahangir Alom[6] proposed an intrusion detection approach based on Deep Belief Networks (DBNs). In this method, features were extracted using a two-layer Restricted Boltzmann Machine. When compared with Support Vector Machines (SVM), the DBN-based IDS showed superior performance and achieved an accuracy of 97.5%.

J. Kim[7] et.al applied a Long Short-Term Memory (LSTM) based Recurrent Neural Network model for intrusion detection using the KDD Cup 1999 dataset. Their study focused on analyzing how different learning rates and hidden layer sizes affect detection performance. After multiple experiments, the model achieved a high detection rate of 98.88%.

Anna L. Buczaket.al[8] and her team emphasized the importance of network data such as packet capture files and NetFlow records in applying machine learning and data mining techniques for intrusion detection. They also highlighted the major challenge of limited availability of labeled datasets in this domain. Additionally, N. Shone[10] and collaborators

proposed a deep learning-based network intrusion detection system that combines machine learning and deep learning techniques. Their model used a non-symmetric deep autoencoder and was tested on the KDD Cup 99 and NSL-KDD datasets, showing effective intrusion detection performance.

3.2 Malware Detection:

Malware is a shortened form of the term *malicious software* and refers to software created with harmful intentions. It is commonly used to carry out illegal activities such as stealing sensitive data, breaking security controls, gaining unauthorized access, or damaging computer systems. Malware represents a wide category of cyber threats that includes programs such as viruses, worms, Trojan horses, spyware, adware, bots, rootkits, ransomware, keyloggers, and backdoors.

Each category of malware consists of multiple families. For instance, ransomware includes families such as Charger, Jisut, Koler, Pletor, RansomBO, Svpeng, and Simplocker. Malware can exist in several file formats depending on the target system. These include UNIX ELF files, Windows Portable Executable (PE) files such as .exe, .dll, and .efi. In addition, malware can be hidden within documents like .doc, .pdf, and .rtf files. It may also appear as extensions or plugins for commonly used platforms such as web browsers and web frameworks.

Dolly Uppal[11] developed a malware detection and classification framework using the n-gram technique. Their approach involved monitoring the execution behavior of malware samples and recording API calls. After constructing feature vectors, various machine learning algorithms were applied, and the Support Vector Machine (SVM) produced the best performance.

Mozammel Chowdhury[12] and his team proposed a malware detection method based on Artificial Neural Networks. They extracted features from PE file headers using the n-gram approach and experimented with an expanded feature set. Their model achieved an accuracy of 97%.

Bowen Sun [13] and collaborators introduced a malware classification model based on static feature analysis from multiple viewpoints. They

extracted features from PE structures, bytecode sequences, and assembly code. Eight different classifiers were evaluated, and the best-performing model achieved an F1-score of 93.56%.

Mahmoud Kalash[14] and his team presented a malware classification approach using Convolutional Neural Networks (CNNs). Malware binaries from 25 different families were converted into grayscale images and used as input to the CNN model. Experiments conducted on the Maling and Microsoft malware datasets showed high classification accuracy of 98.52% and 99.97%, respectively.

3.3 Android Malware Detection:

Android is the most widely used mobile operating system, which makes it a major target for malware developers. As new types of Android malware continue to emerge rapidly, identifying and classifying these malicious applications has become increasingly difficult. Because of this growing threat, many researchers have focused on improving mobile malware detection techniques.

DroidMat [15] applied machine learning approaches such as k-means clustering and k-Nearest Neighbor (K-NN) using static features extracted from Android applications. Several other studies, including those by Arp[16] et al., Varsha et al.,[17] and Sharma and Dash,[18] also relied on static analysis of Android apps. By using machine learning algorithms such as Support Vector Machines (SVM), Random Forest, K-NN, Naive Bayes, and Decision Trees, these approaches achieved effective detection performance.

In contrast, AntiMalDroid[19] and Droid Dolphin[20] focused on dynamic analysis. They extracted behavioral features by monitoring the runtime activities of malware applications and applied Support Vector Machines for classification, resulting in high detection accuracy.

Suleiman Y. Yerima[21] and his team introduced a multilevel classifier fusion approach for Android malware detection. Their method combined multiple classifiers using ranking-based techniques that considered accuracy, recall, and precision. By integrating four different classifiers based on these rankings, the proposed system achieved improved detection performance. The effectiveness of the model was validated using

three different datasets, where it demonstrated a strong recall rate.

3.4 Spam Detection:

Spam detection is one of the important challenges in the field of cybersecurity. Spam refers to unwanted bulk messages that are usually sent for promotional or fraudulent purposes. Although spam is commonly associated with email, it can also appear on social media platforms, blogs, and messaging applications. Such messages not only waste users' time but may also pose serious security risks.

In many cases, spam messages are designed to look like genuine communications from trusted organizations such as banks or service providers. If users respond to these messages or click on malicious links, it can result in significant financial losses or identity theft. Due to these risks, researchers have extensively applied machine learning techniques to automatically identify and filter spam messages.

Muhammad N. Marsono[22] and his colleagues used the Naïve Bayes classification method to detect spam emails among incoming messages and reported effective results. James Clark[23] and his team applied the k-Nearest Neighbor (K-NN) algorithm to address the problem of automated email classification. S. Jancy Sickory Daisy[24] proposed a hybrid spam detection approach that combines Naïve Bayes classification with the Markov Random Field technique. The performance of this hybrid system was evaluated based on accuracy and execution time, and it was shown to outperform basic standalone models.

Sreekanth Madisetty[25] and his collaborators introduced an ensemble-based approach for detecting spam on Twitter. Their work involved developing deep learning models using Convolutional Neural Networks (CNNs). Various word embedding techniques were used to convert text data into numerical representations before training the CNN models. They experimented with five different CNN-based models using embeddings such as Twitter GloVe, Google News, Edinburgh, H- Spam, and Random embeddings, along with one feature-based model for comparison.

Mehul Gupta[26] and his team conducted a comparative study of several machine learning and deep learning methods for SMS spam detection using two different datasets. They evaluated eight classifiers and observed that the CNN-based classifier achieved the highest accuracy of 99.19% and 98.25% on the respective datasets.

Although many studies use a wide range of machine learning models across all four cybersecurity domains, only the most suitable techniques for each problem have been highlighted. Intrusion detection benefits greatly from effective feature selection methods and deep learning models such as Recurrent Neural Networks (RNNs). Traditional malware detection on personal computers is efficiently handled using Artificial Neural Networks (ANNs) and CNNs, where malware samples are often converted into image form before classification. Android malware detection commonly relies on shallow machine learning models and classifier fusion techniques. Spam detection, on the other hand, can be effectively addressed using both shallow machine learning algorithms such as Naïve Bayes and K-NN, as well as deep learning approaches like CNNs.

4. CONCLUSION:

Machine learning techniques are widely used to address different cybersecurity challenges. Recent developments in machine learning and deep learning have introduced effective tools for detecting and preventing cyber threats. However, choosing the right algorithm for a specific security problem is crucial for achieving reliable results. No single model can handle all types of attacks effectively.

To improve detection accuracy and strengthen system security, multi-layered approaches are often required. Such approaches help in building resilient systems that can better withstand evolving malware attacks. The success of a cybersecurity solution largely depends on selecting an appropriate model and applying it correctly.

This study reviewed state-of-the-art methods used to tackle various cybersecurity problems. While machine learning and deep learning models provide powerful automated capabilities, they should not be considered as complete replacements

for human expertise. Combining human supervision with intelligent machine learning techniques leads to more effective and dependable cybersecurity solutions.

ACKNOWLEDGEMENT:

I, **Vijaya Sri M** pursuing a Bachelor of Science in Information Technology Sri Krishna Adithya College of Arts and Science. I presented many papers in various colleges and attended many workshops.

REFERENCES:

- [1] William G Hatcher, Wei Yu, —A Survey of Deep Learning: Platforms, Applications and Emerging Research Trends, IEEE Access 2018, Volume: 6, DOI:10.1109/ACCESS.2018.2830661..
- [2] Venkatesh Jaganathan, Premapriya Muthu Sivashanmugam, Priyesh Cherurveetil, —Using a Prediction Model to Manage Cyber Security Threats, Hindawi Publishing Corporation the Scientific World. Journal Volume 2015, Article ID 703713, <http://dx.doi.org/10.1155/2015/703713>.
- [3] Daria Lavrova, Alexander Pechenkin, Applying Correlation and Regression Analysis to Detect Security Incidents in the Internet of Things, International Journal of Communication Networks and Information Security (IJCNIS), Volume. 7, No. 3, December 2015.
- [4] Saroj Kr. Biswas, —Intrusion Detection Using Machine Learning: A Comparison Study, International Journal of Pure and Applied Mathematics, Volume 118 No. 19 2018, 101-114.
- [5] R. Vinayakumar, Mamoun Alazab, (Senior Member, IEEE), K. P. Soman, Prabaharan Poornachandran, Ameer Al-Nemrat, A.N. Venkatraman, —Deep Learning Approach for Intelligent Intrusion Detection System, IEEE Access, VOLUME 7, 2019, Digital Object Identifier 10.1109/ACCESS.2019.2895334.
- [6] Md. Zahangir Alom, Venkata Ramesh Bontupalli, and Tarek M. Taha, —Intrusion Detection using Deep Belief Networks, 978-1-4673-7565-8/15/\$31.00 ©2015 IEEE
- [7] J. Kim, L. T. Thu and H. Kim —Long Short-Term Memory Recurrent Neural Network Classifier for Intrusion Detection, IEEE International Conference on Platform Technology and Service, 2016.
- [8] Anna L. Buczak and Erhan Guven, A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection, IEEE Communications Surveys and Tutorials, Volume. 18, No. 2, 2nd Quarter 2016.
- [9] Ondrej Kubovič (ESET Security Awareness Specialist), Machine-Learning Era in Cybersecurity: A Step Towards A Safer World or The Brink of Chaos, Machine-Learning Era in Cybersecurity White Paper, February 2019
- [10] N. Shone, V. D. Phai, T. N. Ngoc, Q. Shi, "A deep learning approach to network intrusion detection", IEEE Transactions on Emerging Topics in Computational Intelligence-Feb-2018(41-50).
- [11] Dolly Uppal, Vinesh Jain, Rakhi Sinha and Vishakha Mehra and —Malware Detection and Classification Based on Extraction of API Sequences, 978-1-4799-3080-7/14/\$31.00_c 2014 IEEE.
- [12] Mozammel Chowdhury, Azizur Rahman, Rafiqul Islam, Protecting Data from Mal-ware Threats using Machine Learning Technique, 2017 12th IEEE Conference on Industrial Electronics and Applications (ICIEA).
- [13] Bowen Sun, Qi Li, Yanhui Guo, Qiaokun Wen, Xiaoxi Lin, Wenhan Liu, —Malware Family Classification Method Based on Static Feature Extraction, 2017 3rd IEEE International Conference on Computer and Communications
- [14] Mahmoud Kalash, Mrigank Rochan, Noman Mohammed, Neil D. B. Bruce, Yang Wang, Farkhund Iqbal, —Malware Classification with Deep Convolutional Neural Networks, 978-1-5386-3662-6/18/\$31.00 ©2018 IEEE
- [15] D.-J. Wu, C.-H. Mao, T.-E. Wei, H.-M. Lee, and K.-P. Wu, —DroidMat: Android mal-ware detection through manifest and API calls tracing, in Proc. 7th Asia Joint Conf. Inf. Security (Asia JCIS), 2012, pp. 62–69.
- [16] D. Arp, M. Spreitzenbarth, M. Hubner, H. Gascon, and K. Rieck, —Drebin: Efficient and explainable detection of Android malware in your pocket, in Proc. 20th Annu. Netw. Distrib. Syst. Security Symp. (NDSS), San Diego, CA, USA, Feb. 2014, pp. 1–15.

- [17] M. V. Varsha, P. Vinod, and K. A. Dhanya, —Identification of malicious Android app using manifest and opcode features,|| J. Comput. Virol. Hacking Tech., vol. 13, no. 2, pp. 125–138, 2017.
- [18] A. Sharma and S. K. Dash, —Mining API calls and permissions for Android malware detection,|| in Cryptology and Network Security. Cham, Switzerland: Springer Int., 2014, pp. 191–205.
- [19] M. Zhao, F. Ge, T. Zhang, and Z. Yuan.,|| An efficient SVM- based malware detection framework for Android,|| in Communications in Computer and Information Science, vol. 243, Springer, 2011, pp. 158–166.
- [20] W.-C. Wu, S.-H. Hung, —A dynamic Android malware detection framework using big data and machine learning,|| in Proc. ACM Conf. Res. Adapt. Convergent Syst. (RACS), Towson, MD, USA, 2014, pp. 247–252.
- [21] Suleiman Y. Yerima, Member, IEEE, and Sakir Sezer, Member, IEEE, —Droid Fusion: A Novel Multilevel Classifier Fusion Approach for Android Malware Detection||, IEEE TRANSACTIONS ON CYBERNETICS, VOL. 49, NO. 2, FEBRUARY 2019.
- [22] Muhammad N. Marsono, M. Watheq El-Kharashi, Fayez Gebali, —Targeting spam control on middleboxes: Spam detection based on layer-3 e-mail content classification|| Elsevier Computer Networks, 2009.
- [23] James Clark, Irena Koprinska, Josiah Poon, —A Neural Network Based Approach to Automated E-mail Classification||, Proceedings IEEE/WIC International Conference on Web Intelligence, 0-7695-1932-6, Oct. 2003.
- [24] S. Jancy Sickory Daisy, A.Rijuvana Begum, —Hybrid Spam Filtration Method using Machine Learning Techniques||, International Journal of Innovative Technology and Exploring Engineering, ISSN: 2278-3075, Volume-8, Issue-9, July 2019.
- [25] Sreekanth Madisetty and Maunendra Sankar Desarkar, —A Neural Network-Based Ensemble Approach for Spam Detection in Twitter||, IEEE Transactions on Computational Social Systems, Volume: 5, Issue: 4, Dec. 2018.
- [26] Mehul Gupta, Aditya Bakliwal, Shubhangi Agarwal & Pulkit Mehndiratta, —A Comparative Study of Spam SMS Detection using Machine Learning Classifiers||, Eleventh International Conference on Contemporary Computing (IC3), 2-4 August, 2018, Noida, India, 978-1-5386-6835-1/18,2018 IEEE