Machine Learning in Cyber security

Tanishq Gupta
Scholar
Master Computer of Application
Babu Banarasi Das University
Lucknow, Country
tanishqintern12@bbdu.ac.in

***Abstract*—Data science powers cyber security advancements by using machine learning to detect patterns and build intelligent systems. It addresses issues like phishing, network intrusion, and spam detection. By analyzing data, extracting features, and training models, machine learning enhances security. Regular updates and combining models improve accuracy in detecting evolving cyber threats.**

***Keywords*— Security, Machine Learning, Survey, Machine Learning, Intrusion Detection, Spam Cyber security.**

I. INTRODUCTION

In today's rapidly evolving cyberspace, which serves as a primary medium for node-to-node information transfer, there are both opportunities and challenges. The components of the standard paper have been defined for three main reasons: (1) to simplify the formatting process for individual papers, (2) to ensure automatic compliance with electronic standards, enabling the concurrent or subsequent creation of electronic versions, and (3) to maintain uniform style across conference proceedings. Built-in elements like margins, column widths, line spacing, and typefaces are predefined, with examples provided throughout this document, highlighted in italic and accompanied by clarifying descriptions in parentheses. While certain components, such as complex equations, graphics, and tables, are not strictly prescribed, guidance on appropriate table text styles is provided [6]

II. OBJECTIVE OF THE STUDY

The objectives of this study are to compare and classify various machine learning and data mining methods for cyber threat detection and analysis. It aims to combine multiple analytical techniques into an integrated Cyber Threat Intelligence (CTI) framework and evaluate its efficiency using real-world cyber threat datasets. The study seeks to measure improvements in threat detection accuracy, time, and prevention and to identify key trends and challenges in CTI practice.[2]

In particular, this study seeks to answer the following research questions:
1. Which machine learning algorithms are most effective in addressing different types of cyber threats?
2. What strategies can be used to fuse and prepare the data that originate from multiple sources to enhance threat identification?

3. What trade-offs exist in terms of precision, speed, and interpretability of CTI models?.
4. Finally, How can the results from CTI analyses be effectively applied in managing incidents and countering threats?

III. METHODOLOGY

In the world of cyber security, the use of machine learning techniques has grown in value, allowing for more efficient threat detection and response. The approaches used to use machine learning in cyber security are thoroughly reviewed in this article, with emphasis on their advantages, disadvantages, and practical applications..[4]

A. *Data Collection and Preprocessing Model Selection and Evaluation*

Acquiring relevant data is a critical first step in building effective machine learning models for cyber security, which involves collecting datasets for both training and evaluation. Data cleaning and transformation are essential for ensuring data quality, addressing issues such as missing values and outliers. Additionally, feature extraction and engineering help to identify and select the most relevant features, while also creating new representations that can enhance the model's ability to detect and prevent cyber threats.[2]

B. *Model Selection and Evaluation*

Selecting the right algorithm, like decision trees, support vector machines, or neural networks, depends on the problem and data characteristics. The dataset is divided into training and testing sets to ensure proper evaluation. Model performance is measured using metrics such as accuracy, precision, recall, F1-score, and AUC for effectiveness assessment. [6]

C. *Model Training and Optimization*

Model training involves using supervised, unsupervised, or semi-supervised learning approaches depending on data labeling and availability. Hyper parameter tuning improves model performance using methods like grid search, random search, or Bayesian optimization. Regularization techniques, such as L1 and L2, along with dropout and early stopping, help prevent over fitting and ensure robust models.[7]

D. *Deployment and Integration Phishing Detection*

Real-time monitoring involves deploying models into live systems to detect and respond to cyber threats instantly. These models are integrated with existing security systems, such as firewalls or intrusion detection systems, to enhance protection. Regular updates and maintenance ensure models stay effective by incorporating new data and adapting to evolving threats.[1]

E. *Phishing Detection*

Phishing targets sensitive personal information. Researchers categorize anti-phishing methods into three main groups: **detective methods** (monitoring, content filtering, anti-spam), **preventive methods** (authentication, patching, change management), and **corrective methods** (site takedown, forensic analysis). These approaches work together to detect, prevent, and address phishing threats.[2]

Table 1: Principal Groups of Anti-Phishing Methods

Detective Solutions	Preventive Solutions	Corrective Solutions
□□□ Monitors account life cycle □□□□□□□Brand monitoring □□□□Disables web duplication □□□□□Performs content filteringAnti-Malware □□□Anti-Spam	1. Authentication 2. Patch and change management 3. Email authentication 4. Web application security	□□□□□Phishing site takedown □□□□Forensics and investigation

IV. SYSTEM ARCHITECTURE

Real-time Transaction Analysis System Architecture The overall architectural design of the system is a modular and scalable pipeline that can handle a high volume of transactions at real-time speed. The architecture was designed based on micro services to scale, be fault tolerant and run in real-time.[4]

A. *Data Collection Layer:*

This layer is dedicated to integrating transactional data collected from the checkout page. It collects information like timestamps, keystroke dynamics, sequences of interactions with form fields, IP addresses, device attributes, and transaction frequencies. Secure APIs stream data from client applications in real time.[5]

B. *Preprocessing and Feature Engineering*

Incoming data gets the noise free through preprocessing and

Normalization algorithms on feature engineering derive valuable features such as duration in the forms, order of entered fields, and the identification of users, etc.

C. *Machine Learning Model Layer:*

The following three essential elements make up the ML model layer:

1. **Auto encoder based Anomaly Detection:** Allows auto encoder to find out the anomalous pattern on new transactions using reconstruction error.
2. **K-means or DBSCAN based Clustering**: Groups transaction, flags potential outliers based on the attributes of behavioral features.
3. **Supervised Classification (Random Forest or SVM):** Ear Mark confirms or refutes the detection event (transaction packets) that it flagged, further refining detection[2].

D. *Real-Time Detection Engine:*

This engine serves as the core of the system, handling

transactions in real time. It processes each transaction through the machine learning models and combines their outputs to produce a final detection decision. If a transaction is flagged, security teams or additional verification steps are triggered before finalizing the process [5].

E. *Loggers and Model Update Unit:*

The key to all transactions flagged or Logged for later analysis. It also uses updated data to retrain the models on an ongoing basis to be able to adapt to new attack patterns while ensuring high detection rates [3].

F. *User Interface and Alerting:*

The UI includes a dashboard where security teams can monitor transactions that have been flagged, review alerts in real time and see statistics. Alerts are received by users through email, SMS, or third-party integrations, enabling rapid response[6].

V. IMPACT

Implementing ML-based detection of form jacking significantly enhances security by accurately identifying malicious scripts in real-time. This reduces data breaches, safeguards sensitive user information like credit card details, and minimizes financial losses. The system's adaptability improves threat detection over time, ensuring robust protection against evolving cyber-attacks on online forms.[7]

A. *Proactive Approach*

Unlike traditional tools that respond after a breach, our ML-based solution identifies form jacking attempts before a compromise occurs. This proactive detection significantly enhances security for checkout pages, preventing data theft and reducing the risk of financial or reputational damage for businesses. [4]

B. *Privacy and Security*

Enhanced security builds consumer confidence in online platforms, encouraging safe transactions. This increased trust leads to improved Customer Lifetime Value (CLV) and higher brand credibility. Businesses benefit from loyal customers who feel secure sharing sensitive data, fostering long-term growth and engagement.[3]

C. Cost Reduction:

Automated detection eliminates the need for constant manual monitoring, reducing manpower expenses and operational costs. E-commerce and financial institutions benefit from efficient, cost-effective security that minimizes human error while maintaining robust protection against cyber threats like form jacking.[2]

D. Scalable Solution

The solution is designed to adapt across multiple websites and platforms. Its flexibility allows integration with diverse transaction data and form structures, ensuring scalability and consistent protection, regardless of the organization's size or the complexity of their systems.[3]

VI. USE CASE

Due to the nature of the ML-based form jacking detection system proposed, there are several possible use case scenarios:

1. **E commerce Security:** E commerce transaction security enables immediate assessment of transaction carried out on e-commerce sites, thus protecting user data and minimize risks of foam jacking.[4]

2. **Financial Institutions:** Payment processing companies can make use of this solution to secure online transactions and protect sensitive financial information.[5]

3. **Cyber security Solutions:** The process can be integrated into the security products focusing on the web threats to protect the client-side attacks.[6]

With the rise and growing popularity of machine learning (ML), numerous studies have proposed ML-based solutions for various cyber security tasks, leading to a vast amount of research papers. This wealth of literature has inspired many surveys that aim to aggregate or summarize the state-of-the-art. However, most of these studies tend to focus on a single application, such as cyber risk assessment or IoT security [4], or concentrate on specific cyber detection problems like malware, spam, or intrusion detection. Some studies do not explicitly address ML, while others do not focus on cyber security. Furthermore, many works explore only particular ML paradigms, such as generative adversarial networks, adversarial ML, reinforcement learning, or deep learning. Deep learning, often considered a universal solution, may not always be the most suitable approach for cyber security tasks. This limitation is highlighted in the well-known study by Apprizes et al., which explores the narrower applicability of deep learning in this domain. [3], which has a more limited scope compared to our paper.

(i) focuses on the distinction between shallow and deep learning,

(ii) does not explore cyber security tasks beyond threat detection,

(iii) only considers scientific publications. In contrast, ML has seen significant advancements in cyber security since that study, as we will demonstrate in our work [2].

ACKNOWLEDGMENT

I certify that the thesis titled *Machine Learning in Cybersecurity: Techniques and Challenges*, submitted to the School of Computer Applications, Babu Banarasi Das University, Luck now, is my original work conducted under the guidance of Mohd Asim Sayeed. The work is authentic, has not been submitted elsewhere for any degree or diploma, and acknowledges all sources used.[7]

REFERENCES

[1] Alam, S., Qu, Z., Riley, R., Chen, Y., & Rastogi, V. (2015). DroidNative: Automating and optimizing detection of Android native code malware variants. Computers Tutorials, 18(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2494502

[2] Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques,

systems and challenges. Computers & Security, 28(1-2), 18-28. https://doi.org/10.1016/j.cose.2008.08.003

[3] Grand View Research. (2020). Cyber Threat Intelligence Market Size, Share & Trends Analysis Report By Component, By Deployment, By Organization, By Application, By End Use, By Region, And Segment Forecasts, 2020 - https://www.grandviewresearch.com/industry analysis/cyber-threat-intelligence-market

[4] Kim, J., Kim, J., Thu, H. L. T., & Kim, H. (2016). Long short term memory recurrent neural network classifier for intrusion detection. Proceedings of the International Conference on Platform Technology and Service (PlatCon), 1-5. & Security, 65, 230-246. https://doi.org/10.1016/j.cose.2016.11.011 J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[5] Nisioti, A., Mylonas, A., Yoo, P. D., & Katos, V. (2018). From intrusion detection to attacker attribution: A comprehensive survey of unsupervised methods. IEEE Communications Surveys & Tutorials, 20(4), 3369-3388. https://doi.org/10.1109/COMST.2018.2854724

[6] SANS Institute. (2019). SANS 2019 Cyber Threat Intelligence Survey.https://www.sans.org/reading room/whitepapers/analyst/2019-cyber-threat intelligence-cti-survey-38790

[7] Saxe, J., & Berlin, K. (2015). Deep neural network based malware detection using two dimensional binary program features. Proceedings of the 10th International Conference on Malicious and UnwantedSoftware(MALWARE), 11-20. https://doi.org/10.1109/MALWARE.2015.7413680 interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].