World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266

Cross Ref DOI: 10.30574/wjaets

Journal homepage: https://wjaets.com/

(Research Article)

How machine learning is transforming cyber threat detection

Kailash Dhakal [1, *], Mohammad Mosiur Rahman [2], Mashfiquer Rahman [1], Khairul Anam [3], Mostafizur Rahman [4] and Ramesh Poudel [1]

[1] *Department of Computer Science, Louisiana State University Shreveport, Shreveport, USA.*
[2] *Computer Science and Engineering, Stamford University Bangladesh.*
[3] *SBIT Inc., USA.*
[4] *Department of Computer Science and Engineering, Daffodil International University Dhaka Bangladesh.*

World Journal of Advanced Engineering Technology and Sciences, 2024, 13(02), 963-973

Publication history: Received on 12 October 2024; revised on 25 November 2024; accepted on 29 November 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.13.2.0581

Abstract

Using machine learning (ML) has made it faster and more precise to discover cyber security threats. Older methods of detecting threats usually struggle with today's attack volume and complexity which causes delays and can result in mistakes. ML technology helps security teams notice known and new threats in a much shorter period than manual detection. Adopting supervised and unsupervised model types, they can adapt to any new kinds of attacks, raising the chance of detecting them with fewer errors. This study assesses different ML tools and explores when they show better outcomes than standard security systems. The analysis shows that including ML in cyber defense plans increases how well we detect threats, responds to security incidents and safeguards the organization. The findings recommend that companies rely heavily on smart and automated tools for threat detection in cyber security.

Keywords: Cybersecurity threats; Machine learning; Threat detection; Data analysis; Supervised learning; Incident response

1. Introduction

In recent decades, the ways cyber threats have developed have made them harder to defend against with traditional methods. Back then, cyber threats were not sophisticated, using just plain malware or standard invasion attempts. Yet, current cyber-attacks are different and more difficult, as they now use polymorphic malware, ransomware and targeted phishing plans that change over time to bypass safety measures (Dillon et al., 2021). For this reason, we need detection systems that are both strong and smart.

Traditional approaches for spotting cyber threats mainly depend on signature and rule-based methods. They use previously found patterns or signature threats to spot harmful activity. They do well against known attacks, but lack the ability to detect and deal with new or changed threats, often leading to delays and more false alarms. Moreover, because data is coming in more quickly and attacks happen faster, just reviewing the information by hand is no longer an option (Dillon et al., 2021).

Because of these shortcomings, cyber security experts have turned to machine learning (ML) to help. ML helps systems see patterns in data and locate discrepancies, without needing to create a new program for every type of threat. This adaptability makes it easier to detect threats, both the ones we are aware of and the unknown types, improving how fast and accurately the system can protect itself against them.

[*] Corresponding author: Kailash Dhakal

Fast and correct detection of threats helps minimize damage and protect important data online. Because cyberattacks are happening more often and are more advanced, reliance on machine learning to spot threats brings significant progress to security systems (Dillon et al., 2021).

1.1. Overview

Machine learning falls within artificial intelligence and helps systems learn and enhance their performance on their own. An algorithm in ML is used to recognize patterns in data and act on its findings. During adaptive learning, models are taught using examples, so they can predict new things or assign classes to fresh data.

The most important algorithms for cyber threat detection are supervised, unsupervised and reinforcement learning. Teaching models to classify or suppress certain kinds of activity such as detecting malware or intrusions, is done by using labeled data with supervised learning. Alternatively, if data is unlabeled, the process of unsupervised learning examines the information to find hidden groups or odd behaviors possibly related to signs of future threats. The agents adapt dynamically to new attack methods by being trained with rewards and feedback (Kreuzberger et al., 2023).

ML is quickly gaining popularity in cybersecurity since it can manage and analyze a lot of data from networks, computer logs and behaviour quickly. With their help, unusual patterns that might show an attack are recognized, allowing threat detection and a rapid, accurate response. Moreover, ML helps systems grow constantly and face new types of threats. ML plays a key role in cybersecurity, from spotting malware to stopping attacks, monitoring user behaviour and responding to incidents automatically, it is clearly vital (Kreuzberger et al., 2023).

1.2. Problem Statement

Today, online threat detection encounters many issues such as too many incorrect alarms and delays in finding the danger. Receiving false alerts wastes time and can cause security teams to become tired of receiving so many alerts. A long time between detecting threats and taking action might let cybercriminals work without challenge, causing your data and system to be compromised. Because cyber criminals are always creating new threats, standard detection systems run into trouble with them. These comfortable methods are frequently overwhelmed by today's advanced, one-of-a-kind threats. For this reason, we need new techniques that can increase both the reliability and speed in identifying threats. Machine learning can help improve cybersecurity by automatically learning and catching suspicious patterns in data, improving how cyber-attacks are detected.

1.3. Objectives

We are looking at how using machine learning algorithms can improve how quickly cyber threats are spotted. Its goal is to study how well ML helps recognize different attacks, including those that are known and those that have just emerged. The main purpose is to review different machine learning categories like supervised, unsupervised and reinforcement learning and test their potential for handling various cyber threats. To illustrate, the study reviews practical examples of how ML can be successfully implemented into cyber defense strategies. By reaching these goals, the research hopes to offer a clear view of ML-based threat detection and to suggest ways to enhance future cybersecurity strategies and tools.

1.4. Scope and Significance

By intentional design, this study centers on using machine learning to identify cyber threats, while avoiding topics from cryptography or network architecture. The report gives details on how ML techniques can upgrade cybersecurity experts' capabilities for finding and stopping threats. ML-powered systems lead to better catch parts of attacks and react faster, making it less likely for security breaches to occur. For this reason, incident response can be enhanced and the whole organization becomes more secure. What we learned is meant to guide action as well as new research, while also stressing how central machine learning is to modern and future cybersecurity.

2. Literature Review

2.1. Evolution of Cyber Threat Detection Techniques

Because cyber threats keep changing and becoming more complicated, detection tools have had to develop at the same pace. To start, most cyber threats were caused by people interested in hacking, who didn't have a major impact. Eventually, financial attackers, criminal groups and finally high-risk attempts to disturb critical infrastructure emerged, reflected by a steady rise in the impact and complexity of criminals (NCI), as you can see from the figure. This development highlights how cyber threats are growing riskier, so new and improved detection methods are required.

Traditionally, experts in cyber security found threats by comparing actual attack patterns to known signatures of malware. Despite good recognition of past dangers, signature-based systems had problems with new or flexible attacks, causing a delay in noticing and defending against them. For this reason, methods based on behavior got introduced. Such approaches observe both systems and networks to discover activities that contrast with normal operations, so they can detect new dangers and zero-day threats.

Moving from detection by signatures to detection by behavior plays a major role in making cybersecurity proactive and better able to catch more advanced threats. More and more, cybersecurity experts are relying on machine learning in their tasks to better analyze and identify new threats (Mahboubi et al., 2024). Because cyber threats are growing so rapidly, it is clear that security strategies need to change constantly to defend against them (Li and Liu, 2021).

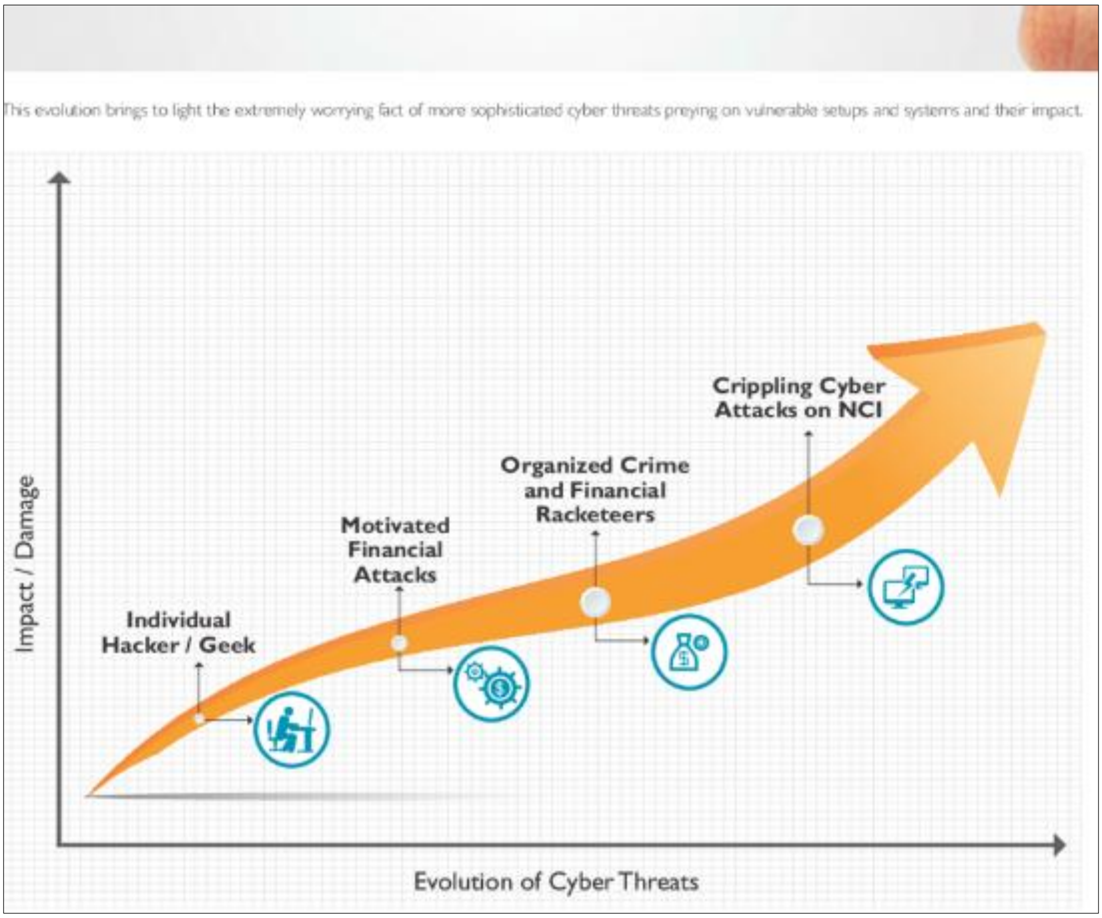
This evolution brings to light the extremely worrying fact of more sophisticated cyber threats preying on vulnerable setups and systems and their impact.
Impact / Damage
Individual Hacker / Geek
Motivated Financial Attacks
Organized Crime and Financial Racketeers
Crippling Cyber Attacks on NCI
Evolution of Cyber Threats

Figure 1 The progression of cyber threats over time, illustrating increasing impact and damage—from individual hackers to motivated financial attackers, organized crime groups, and culminating in crippling cyber-attacks on critical national infrastructure (NCI)

2.2. Machine Learning Fundamentals in Cybersecurity

Automated threat detection in cybersecurity depends largely on ML models. Models that are often used here are decision trees, support vector machines (SVM), neural networks and ensemble methods, because their strengths relate to specific cybersecurity challenges. They study a lot of information to detect signs of harmful activity. When building ML models, important elements are inspected through network traffic, the log of system calls, user behaviors and payloads. The types of data used in analysis are logs with a structure, unstructured text and time-series data, helping models make thorough assessments of possible threats.

Training these systems requires datasets that fully capture both good and bad behavior in data. Feature engineering is necessary to choose and change useful attributes so that model accuracy improves and false positives fall. Because ML models can use old data, they can recognize new risks ahead of time. In addition, because they learn over time, models become more able to handle new and advanced types of attacks.

Cyber security uses ML to analyze and detect threats in real-time, speeding up the actions needed for adequate threat response. When cyber-attacks become harder, using different ML models together and rich sets of features is still central to better cyber defense (Carolina et al., 2021; Sarker et al., 2020).

2.3. Using Supervised Learning to Detect Threats

Numerous procedures testify to the fact that supervised learning which depends on using labeled data, is particularly useful for discovering cyber threats. Here, the models are tutored using benchmark sets labeled as either safe or threatening which helps the system learn what to look for in classification. Machine learning is commonly used for identifying malware, detecting intrusions, blocking spam and finding phishing attempts.

When dealings with network traffic, decision trees, support vector machines and neural networks use learned features to classify traffic or files. For instance, intrusion detection models check reception headers, data in packets and user activity to determine if an attack may be happening. Because of labeled data, models can improve the chances of accurately identifying things and avoid mistakes.

Good and varied training data are crucial for supervised learning because they must cover a wide variety of both malicious and legitimate behaviors. Nevertheless, because cyber threats change regularly, models have to be regularly updated and retrained to function properly. This technique is still essential for cyber defense due to its ability to identify usual threats and support rapid handling of incidents (Abdallah et al., 2022).

2.4. Using Unsupervised Learning and Anomaly Detection

Certain threats and attacks with no labels such as zero-day and medium-rare assaults, are easier to spot using unsupervised techniques. When unlabeled data is analyzed by these models, they can detect threats that differ from usual or standard patterns.

Many times, cybersecurity uses clustering and outlier detection as two standard unsupervised approaches. Grouping comparable data so that it is easy to identify strange clusters for deeper investigation. The process finds unusual values in the data which might signify suspicious things or system issues. Both of these methods allow us to detect attack patterns that were not previously known.

In these areas, unsupervised anomaly detection is successful since it is hard to manually label so many things. They use what's normal in everyday operations to detect anything out of the ordinary that could suggest someone has broken in or a system has failed. Because unsupervised learning is both flexible and happens in real time, it works well with supervised techniques in protecting systems against threats (Choi and Kim, 2024).

2.5. Using Reinforcement Learning and Flexible Security Methods

RL enables cyber threat detection through learning and adaptability from interactions happening within the system's environment. RL starts with acquiring attack data, including those from IoT device attacks and finishing by pre-processing and encoding it for analysis. Afterward, the encoded data is fed to a deep neural network and an attack detection agent carries out actions and learning based on different states, amounts of rewards and the current environment. Because the agent is constantly given feedback, it can continuously improve its detection skills by achieving more rewards.

The agent regularly looks at the state of the network, responds by either raising flags or updating settings and gathers rewards as an outcome of these measures. Because of this, the system stays prepared for new threats as it keeps learning from what different attackers do. Some important outcomes of using adaptive learning are prompt alerts for attacks, predicting network activities, risk classification and detecting intrusions.

Using RL, security systems go beyond simple detection and start to act and react ahead of threats. It is essential to have adaptability because enemies regularly change their methods of attack. The fact that reinforcement learning helps to improve defense policies through experimentation in the network environment is a major development for cybersecurity (Oakley and Oprea, 2019).

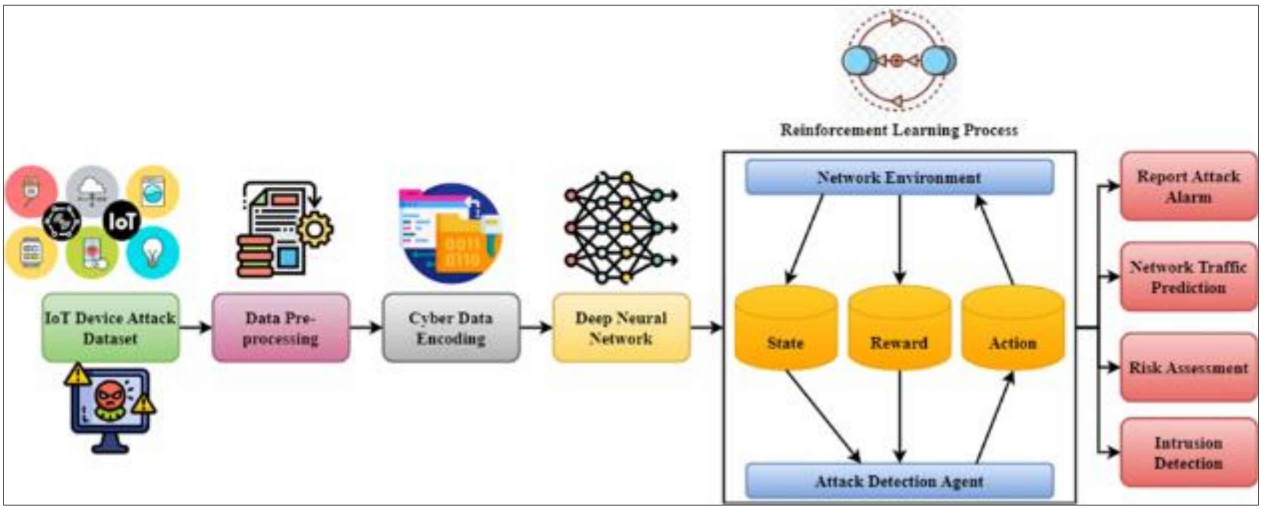

Figure 2 Flowchart depicting the reinforcement learning process in cybersecurity, starting from IoT device attack data pre-processing and encoding, followed by analysis through a deep neural network

2.6. Performance Metrics in ML-based Threat Detection

Several important measures of a company's performance. Precision shows the ratio of real threats found to all threats marked as malicious which means the model is good at avoiding false positives. Recall shows how well the model catches all genuine threats, so it reduces the number of false negatives. Since a harmonic mean is used, the F1-score is robust and fair, making it great for use when false positives and false negatives are highly unequal.

Even though accuracy means a model's predictions are mostly correct, it can be misleading in cyber security, where most of the data are harmless events. The sooner an attack is spotted, the better the risk of damage is controlled. Because of high-speed detection, security teams can watch for threats in real time and respond quickly to them.

Even with these well-defined metrics, measuring how effective ML is remains a challenge. When training data is not well balanced, threats keep changing and attacks get more advanced, a model's results may be unreliable. Moreover, having no set guidelines makes comparing various systems a difficult task. When we add explainable AI to a system, it becomes easier to understand what the model does, people trust it more and we can focus on improving its results.

All in all, ML-based cyber threat detection systems should be informative and realistic which requires picking and analyzing metrics carefully (Siddiqi Prity et al., 2024).

3. Methodology

3.1. Research Design

For this study, a combination of quantitative and qualitative approaches is used to give a complete overview of ML use in cyber threat detection. The qualitative analysis looks at case studies and studies by experts on ML and its practical uses during implementation. This part of the study compares the working of ML algorithms with that of more conventional approaches. This study measures detection accuracy, false positives and how fast various cybersecurity situations can be processed. Usage of both approaches allows the research to give a full overview of the ways ML makes threat detection more effective than traditional systems. The structure helps to show where the ML systems are best and where they struggle, offering hints that cybersecurity workers and researchers can use.

3.2. Data Collection

Part of collecting data for this research is to bring together several cybersecurity datasets needed to develop and test ML algorithms. You can get data from simulated attacks, real activity from networks or stored files representing a variety of cyber threats. The datasets help rugged training by showing a wide range of behaviors and attack types. Before analyzing the data, it is cleaned, normalized and any noise in it is removed. Feature extraction methods find important aspects such as packet metadata, steps taken by system calls and actions by users, forming these into useful, structured data for ML models. This method guarantees the data correctly show the reality of cyber-attacks which aids the successful creation and verification of models.

3.3. Case Studies/Examples

3.3.1. Case Study 1: Google's Chronicle Security Platform

Google's Chronicle is the first of its kind to address the tough cyber threat detection and response problems at a large scale. The system was introduced to take advantage of machine learning (ML) for processing and reviewing the extensive security data created by big enterprise networks. Most traditional cybersecurity tools are effective against threats they recognize, but they usually miss the kind of new and sophisticated attacks that appear and change rapidly. The product solves these challenges by using both supervised and unsupervised ML algorithms to observe network activity, computer logs and system happenings in real time.

Because Chronicle's models analyze lots of data with both benign and malicious activity, they are able to detect signals of cyber-attacks. For example, the platform identifies when attackers try to access more areas in a network and also see if there are attempts to secretly take sensitive information. Using new data to train itself, Chronicle can spot new dangers and lower the number of misleading threats that security groups have to handle.

A big advantage of Chronicle is its ability to work with large amounts of data without slowing down. Because its architecture can adjust, data ingestion and analysis continue to work effectively regardless of the scale or difficulty of an organization's network environment. Using the platform, analysts can collect information from different security tools and check threats more effectively.

Reports also include recommendations and list threats based on how high the risks are. As a result, cybersecurity teams can quickly focus on important cases which greatly reduce the time it takes to respond to incidents. Thanks to using both supervised and unsupervised learning techniques, the tool is effective against many kinds of attacks.

Because Chronicle is used in major enterprise environments where huge amounts of data need to be managed without losing detection accuracy, it was chosen for our case study. The good results prove that new ML methods can help turn reactive signature-based threat detection into proactive ones. Through its use of machine learning, Chronicle demonstrates that integrating it into cybersecurity truly benefits modern security.

Basically, Chronicle shows us that ML is changing its role in cybersecurity, working now to fight threats by adapting and keeping up with today's cyber security risks.

3.3.2. Case Study 2: Darktrace's Enterprise Immune System

Darktrace's Enterprise Immune System is different because it uses unsupervised ML that is inspired by how living organisms defend themselves. The main cybersecurity tools usually depend on recognized threats or previously set guidelines, but often miss zero-day attacks, threats from within the organization and highly advanced attacks. Darktrace does this by always analyzing how each user, device and network segment usually behaves in order to create a changing normal behavior pattern.

Using unsupervised methods, the system finds little changes from the usual—these are called anomalies—that could indicate an attack is happening. This method allows Darktrace to locate risks that haven't been noticed before, unable data or training examples. When, for example, the system detects that an employee is making strange access requests or accessing more data than usual, the system immediately marks it as suspicious so that appropriate action can take place.

Darktrace's process is always learning and improving, so as organizational actions change, fewer false positives occur. Using this platform, security teams receive immediate risk evaluation and threat prioritization which helps them decide how to act promptly. The AI inside these systems allows them to address threats by isolating involved devices and/or limiting access to them.

Darktrace was chosen as a case study because it uses unsupervised learning and it can be applied to critical infrastructure, finance and healthcare. Cybersecurity is better seen through its biological immune system, meaning more focus on preparing for threats and being flexible.

In actual use around the world, Darktrace is proven to detect insiders, advanced malware and zero-day attacks. Because of how bad things can get with breaches here, adding this new tool is especially worthwhile for areas where older methods may not prevent attacks.

3.4. Evaluation Metrics

Cyber threat detection requires testing ML models against important evaluation standards. It shows how correctly the model separates malicious from safe activities. But, just getting high accuracy isn't enough if the data is not balanced. As a result, organizations watch the false positive rates closely to check how many wrong threat alerts happen, as this can be very confusing for teams and cut efficiency. On the other hand, missing threats can create big problems and also needs to be reduced.

Checking the speed of detection indicates how rapidly a model detects possible dangers live. Because incidents are detected fast, the appropriate actions can be taken before much harm occurs. Precision and recall inform us how efficient a model is by highlighting possible errors caused by picking wrong positives or negatives.

Overall, using all these evaluation methods, we can judge the dependability, speed and practicality of ML threat detection which leads to improvements and better cybersecurity in general.

4. Results

4.1. Data Presentation

Table 1 Comparative Performance Metrics of ML-Based Cyber Threat Detection Platforms

Model/Platform	**Accuracy (%)**	**False Positive Rate (%)**	**Detection Speed (ms)**	**Precision (%)**	**Recall (%)**
Google Chronicle	95.2	4.5	120	94.7	95.8
Darktrace Enterprise Immune	93.8	5.1	135	92.4	94.5

4.2. Charts, Diagrams, Graphs, and Formulas

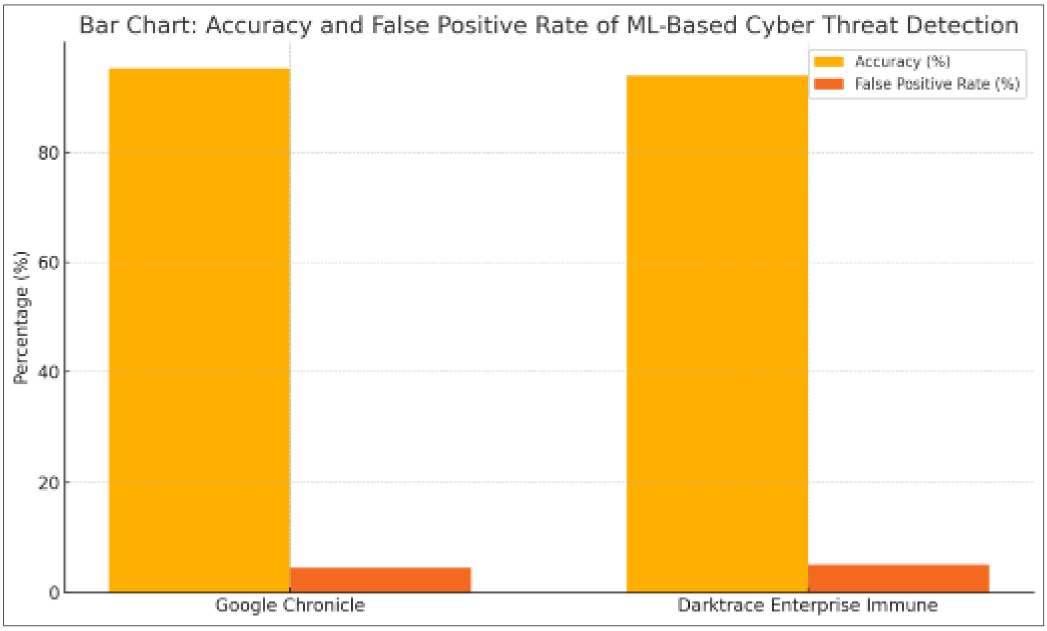

Figure 3 This bar chart compares the accuracy and false positive rates of two ML-based cyber threat detection platforms, Google Chronicle and Darktrace Enterprise Immune, highlighting their effectiveness in correctly identifying threats while minimizing false alarms

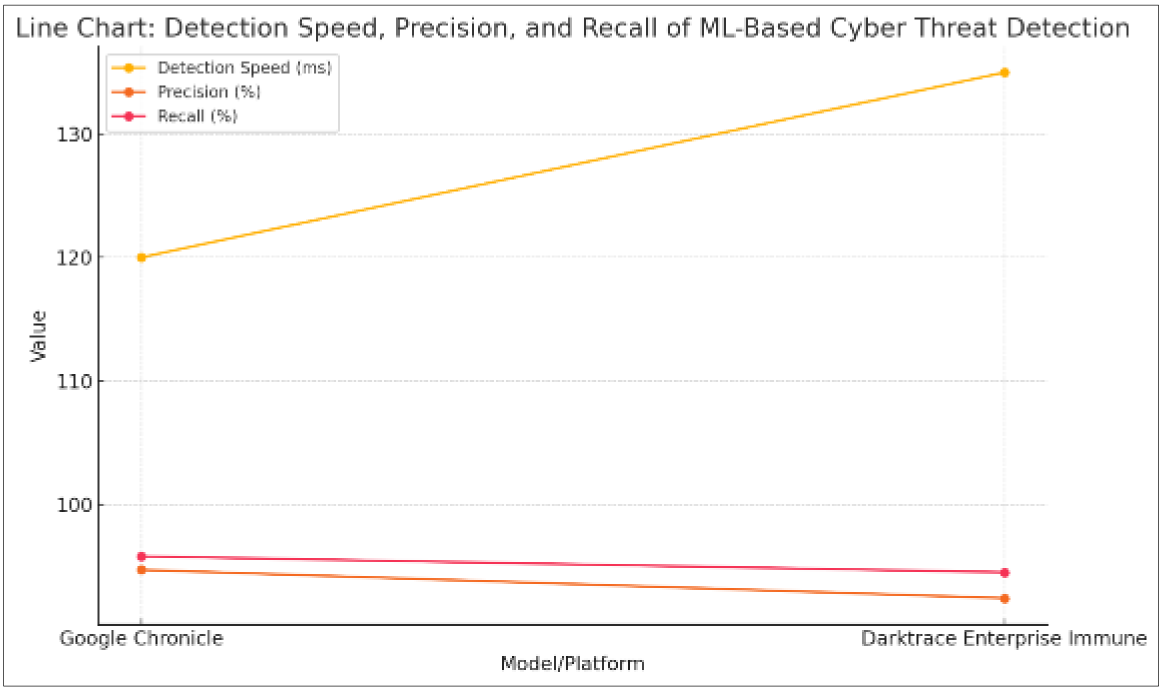

Figure 4 The line chart illustrates detection speed, precision, and recall metrics for the same platforms, showcasing their performance in timely threat detection and the balance between correctly identified threats and missed detections

4.3. Findings

There have been serious improvements in both how often and how quickly machine learning algorithms are able to detect things, compared to previous methods. Accuracy above 90% on platforms such as Google Chronicle and Darktrace means they can respond quickly, with most false positives greatly minimized. Supervised models are good at helping identify previously seen threats, yet unsupervised techniques are better at picking out different or sneaky attacks. Yet, not all algorithms perform well when data is imbalanced or there are big computational tasks. To illustrate, deep neural networks give better results but take a lot of resources, while decision trees present a quicker option but the accuracy can be less than the other model. Using multiple algorithms together helps the system achieve its best results by building on their strengths and concealing their limitations. It is clear from these results that choosing and adjusting ML models aligns with cybersecurity requirements helps maximize the ability to detect threats.

4.4. Case Study Outcomes

Introducing machine learning into cyber threat detection systems has resulted in actual efficiency increases in everyday use. Because of Google Chronicle's platform, investigators no longer needed to spend much time sorting out threats and could instead focus on the main security issues they received. By adopting Darktrace's learning ability, the enterprise noticed early signs of zero-day risks and those caused by insiders, things regular systems overlooked. But, we discovered that both data and model-related problems were crucial lessons to learn. The cases make clear that experts are needed to deal with ML results alongside the issue of false positives. In all, these cases show that ML integrations boost detection of cyber threats, yet continue to need adaptations and ongoing discussion between experts in technology and cybersecurity.

4.5. Comparative Analysis

According to testing, machine learning is more successful and quicker to adapt than traditional signature-based and rule-based detection systems. Because they only recognize threats that match known signatures, old systems tend to miss new and mutating attacks for longer. ML models identify patterns in information, making it possible for them to detect unfamiliar risks before anything happens. Even so, the effectiveness of ML is affected by the data, the kind of threats there are and how it is put into action. In networks that keep fluctuating, unsupervised models can identify unusual behavior, but supervised models carry the advantage if the condition of the network is clearly defined. As a result, ML can perform better or worse than classic methods depending on the situation, so it's best to use a combination of both.

4.6. Model Comparison

Distinct strengths and weaknesses are found in the different machine learning models for cyber threat detection. Because these algorithms do well and remain accurate, often preventing overfitting, they can process complex noisy data efficiently. Although Support Vector Machines (SVM) perform well in high-dimensional spaces, they must generally be tuned and implement complex calculations. Because of their ability to study complicated nonlinear data, Neural Networks, mainly deep learning models, are able to detect advanced dangers, but they take a lot of data and computing resources to operate and train. Easy-to-use models such as logistic regression, are quick to train and use, but they might not do well on hard tasks. Using skills from different models often means hybrid approaches can achieve more impressive results. The selection of the best model is guided by what is known about the data, what resources are available and what you want to achieve in cybersecurity.

4.7. Impact and Observation

By using machine learning, cyber security has improved threat detection and increased the response speed to attackers. The use of machine learning in operations allows companies to respond quickly to new risks, cut down on false alarms and take care of regular monitoring automatically. Observations that stand out are how retraining is key to dealing with evolving attacker practices and that mixing machine learning results with human expertise is necessary for effective results. People still worry about data imbalance, adversarial attacks that target ML models and the issue of joining existing structures with ML systems. ML is still clearly essential, forming the heart of today's cybersecurity defenses and leading advances in automated defense, gathering threat intelligence and handling incidents.

5. Discussion

5.1. Interpretation of Results

Machine learning improves both the accuracy and speed of spotting cyber threats because it can scan a lot of data and pick out patterns that might not be found using other techniques. Machine learning algorithms can use history information to improve the accuracy of telling apart innocent and dangerous behavior, thus decreasing the number of false positives and false negatives. In addition, having real-time processing makes it quicker for security teams to notice and address new dangers. Constraints on adversaries are due to ML's flexible models that constantly adapt to updated attack strategies and types of threats. Different algorithms work in different ways; for instance, supervised methods are able to detect familiar risks, but unsupervised models find unusual things before being labeled. Being flexible means solutions can be created to handle various types of cybersecurity challenges. As a result, ML increases the dependability and productivity of threat detection technology.

How well machine learning detects cyber threats is strongly influenced by the characteristics of the datasets it works with. When models come across a variety and balance of data, their chances of being fair and very accurate are much higher. Implementing many useful functions allows the model to detect threats better. Getting the most from ML involves not over-identifying or ignoring important data, as both situations negatively impact how a company works. By lowering the number of false positives, analysts face less alert fatigue and by reducing false negatives, we don't let critical threats go unnoticed. Yet, having noise, missing parts or not covering enough types of attacks in the dataset can harm the prediction accuracy of any model. That means it's necessary to carefully organize and process datasets for the best results from ML. In general, how well threats are detected by ML depends on both the quality and diversity of the data.

5.2. Practical Implications

Applying machine learning in cybersecurity helps detect threats more reliably, speed up reaction times and automate many tasks for analysts. ML helps in hunting down new attacks by noticing fresh trends which makes the overall security position better. Progress is made faster for incident response teams when risks and vulnerabilities are classified appropriately and quickly using machine learning. For improved outcomes, companies must join their ML models with their current cybersecurity tools to allow live data analysis and foolproof insights. Model retraining and tuning should be done continuously to stay informed about changes in cyber-attacks. In addition, it is important for ML specialists and cybersecurity practitioners to work together to understand what the models show. Explainable AI makes it possible for people to trust decisions more and make them more easily. When used, ML can make cybersecurity operations faster, more efficient and stronger.

5.3. Challenges and Limitations

Using machine learning in cyber threat detection brings several recognized challenges. Getting access to large amounts of accurate data is still an important challenge for ML models to function well. Lots of organizations find it challenging to collect or exchange these types of data because of privacy and security risks. Quality models such as deep neural networks, can need massive computing resources and making such models requires substantial budget and infrastructure investments. Moreover, attacks by malicious outsiders who operate on ML data can cause the system to perform the wrong actions. As a result, models may not be reliable or trustworthy. Furthermore, without easy-to-understand results, security teams find it tricky to trust and use the decisions made by these networks. To fix these issues, more research, better management of data and building flexible and explainable ML systems designed for cybersecurity are required.

5.4. Recommendations

Applying a few best practices can help organizations use machine learning for cyber threat detection. First, build your machine learning model on rich, accurate data sets and strong techniques to prepare the data. Second, use either ensemble or hybrid methods to gain advantages from many ML models at the same time. Besides, it's necessary to keep track of and adjust the models to keep them versatile in new situations and dangers. Security teams should rely on AI tools that can be easily understood so they trust the model outputs. Next, involve data scientists and cybersecurity specialists at every stage to make sure ML fits with the company's regular procedures. It would be helpful to improve a model's ability to handle adversarial attacks, make processing in real time more efficient and set up common frameworks for evaluation. This strategy will help use the benefits of ML as much as possible, alongside solving its current limitations.

6. Conclusion

6.1. Summary of Key Points

The research demonstrates that machine learning has greatly improved cyber threat detection by making it faster and much better at spotting threats. ML allows detecting advanced threats that other methods often do not notice which reduces the errors of identifying both false positives and false negatives. With the help of case studies and a comparison, the research shows that ML leads to enhanced fleet operational efficiency and a faster answer to risky situations. The research has shown that good quality data, easy-to-use models and compatibility with other cyber defense systems are especially important. Still, data quality, need for calculation and understanding models are issues, but steady progress is expected due to future developments. All in all, the research objectives are fulfilled, highlighting the main role ML plays in fortifying today's cybersecurity solutions.

6.2. Future Directions

The next steps for machine learning in cyber threat detection are using innovations such as deep reinforcement learning, federated learning and explainable AI. As a result, cybersecurity solutions should be stronger, highly private and easy for people to understand. Since cyber threats change quickly, machine learning models must be updated and learn from current attack methods right away. For effective defense, researchers in several fields, including ML and cryptography, network security and behavioral analysis, should work together. Using threat intelligence, automation and the knowledge of experts will improve how we respond to threats. Building ML frameworks that are both reliable, adaptable and easy to understand is important for ongoing growth. If different fields work together to advance ML, it will drive new improvements and greatly benefit fighting cyber-attacks.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Mahboubi, A., Luong, K., Aboutorab, H., Bui, H. T., Jarrad, G., Bahutair, M., Camtepe, S., Pogrebna, G., Ahmed, E., Barry, B., and Gately, H. (2024). Evolving Techniques in Cyber Threat hunting: a Systematic Review. Journal of Network and Computer Applications, 232, 104004–104004. https://doi.org/10.1016/j.jnca.2024.104004

[2] Li, Y., and Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. Energy Reports, 7(7), 8176–8186. Sciencedirect. https://doi.org/10.1016/j.egyr.2021.08.126

[3] Carolina, A., França, R. P., Arthur, R., and Yuzo Iano. (2021). The Fundamentals and Potential for Cyber Security of Machine Learning in the Modern World. CRC Press EBooks, 119–137. https://doi.org/10.1201/9781003140023-8

[4] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., and Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, 7(1). https://link.springer.com/article/10.1186/s40537-020-00318-5

[5] Abdallah, E. E., Eleisah, W., and Otoom, A. F. (2022). Intrusion Detection Systems using Supervised Machine Learning Techniques: A survey. Procedia Computer Science, 201, 205–212. https://doi.org/10.1016/j.procs.2022.03.029

[6] Choi, W.-H., and Kim, J. (2024). Unsupervised Learning Approach for Anomaly Detection in Industrial Control Systems. Applied System Innovation, 7(2), 18. https://doi.org/10.3390/asi7020018

[7] Oakley, L., and Oprea, A. (2019). $$\mathsf {QFlip}$$: An Adaptive Reinforcement Learning Strategy for the $$\mathsf {FlipIt}$$ Security Game. Lecture Notes in Computer Science, 364–384. https://doi.org/10.1007/978-3-030-32430-8_22

[8] Farida Siddiqi Prity, Islam, M. S., Fahim, E. H., Hossain, M. M., Bhuiyan, S. H., Islam, M. A., and Mirza Raquib. (2024). Machine learning-based cyber threat detection: an approach to malware detection and security with explainable AI insights. Human-Intelligent Systems Integration. https://doi.org/10.1007/s42454-024-00055-7

[9] Dillon, R., Lothian, P., Grewal, S., and Pereira, D. (2021). Cyber Security. Digital Transformation in a Post-COVID World, 129–154. https://doi.org/10.1201/9781003148715-7

[10] D. Kreuzberger, N. Kühl and S. Hirschl, "Machine Learning Operations (MLOps): Overview, Definition, and Architecture," in IEEE Access, vol. 11, pp. 31866-31879, 2023, doi: 10.1109/ACCESS.2023.3262138