World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

The role of AI in predictive cybersecurity

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

[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, 2022, 06(02), 147-157

Publication history: Received on 13 June 2022; revised on 26 July 2022; accepted on 28 July 2022

Article DOI: https://doi.org/10.30574/wjaets.2022.6.2.0094

Abstract

This research investigates how Artificial Intelligence (AI) supports predictive cybersecurity by analyzing behavior to recognize and block upcoming cyberattacks. Due to the increasing difficulty of cyber-attacks, age-old reactive approaches to cybersecurity are inadequate. The research relies on machine learning algorithms and behavioral analytics to test their ability to find anomalies and predict attacks. After observing data, conducting case studies, and reviewing models, the study finds that AI can make early threat detection more accurate, lower the number of false alarms, and quicken response times. The study found that AI can bolster cybersecurity systems by bringing forward automatic defenses. It is argued in this paper that including AI-powered predictive approaches in system security can make them more efficient and safe. Results suggest areas where further study can help AI prediction systems work better and process more cases.

Keywords: AI cybersecurity; Predictive analytics; Behavioral analytics; Threat detection; Machine learning; Anomaly detection

1. Introduction

The number and complexity of cyber-attacks have increased, with more threats targeting critical infrastructure, firms, and people. Malware can appear differently; ransomware is increasingly used, and individuals are exploited in social engineering, making conventional cybersecurity strategies less effective. With the rise in more advanced threats, we must switch to proactive cybersecurity to stop attacks before damage occurs. Cybersecurity has seen great changes due to Artificial Intelligence (AI) since it can review enormous datasets, understand patterns, and foresee challenges more precisely and quickly than earlier methods. Continuous monitoring and adaptive reaction are key for protecting networks against tricky cyber threats. One promising idea is using predictive cybersecurity, which looks for unusual actions by users and systems to spot dangerous threats. Looking for unusual behavior changes, AI software can't detect security threats and provide advanced protection before they impact the system. Being proactive in cybersecurity has boosted its performance, switching the emphasis from incident response to planning for threats while the attack window is closed. As the risks from cyber threats rise, adding predictive analytics with AI to cyber defense frameworks helps organizations secure their digital resources.

1.1. Overview

This article examines how AI improves cybersecurity predictions using behavioral information. It started by introducing the research and the main goals, followed by a study of current AI applications in cybersecurity in the literature. The

* Corresponding author: Kailash Dhakal

methodology chapter describes how the study was designed, collected data, and calculated scores to assess AI-driven predictive methods. Later chapters analyze the data and present cases, discussing what the findings mean and what recommendations should be made. In the last section, the study highlights what was learned and suggests where future studies could go. At the heart of this research are three basic ideas: AI models, predictive analytics, and behavioral analytics. AI models describe the computer methods—like machine learning and deep learning—that help discover data trends and predict results. With the help of predictive analytics, organizations use current and past data to decide where and when cyber-attacks are likely to happen so they know how to protect themselves. Any changes in user or system behavior that happen quickly are noticed by behavioral analytics to help find suspicious activity. As a result, predictive AI in cybersecurity helps shield networks by upgrading and adapting as security threats appear. Using this method leads to more accurate discoveries and fewer false positives, which help with how efficiently and securely operations are run (Nourani, 2021).

1.2. Problem Statement

Most customary cybersecurity strategies handle threats only after they have arisen. Delaying recovery exposes systems to major issues, information loss, and business disruptions. Detecting cyber threats is still difficult because modern attackers can sometimes get past common detection tools. Early prevention matters, but today's technology often has many false positives and isn't good at predicting problems. Still, we are not fully using AI to predict and prevent cyber-attacks reliably. Not every organization builds AI models for anticipation because of skills, tools, or data quality data quality issues. There is a strong need to find AI-based methods that analyze data on online behaviors to help detect risks and advance cyber security in advance.

1.3. Objectives

In this study, we investigate machine learning models that predict cyberattacks by studying how people interact online. It requires looking at different machine learning and deep learning methods that spot abnormal activity that might signal a potential danger. Besides, the research will examine how well and accurately these cybersecurity methods perform, review their advantages and disadvantages, and evaluate whether they can be used in practice. We also strive to look into real cases where AI was successfully used to foresee cyberattacks to guide our strategies and overcome future roadblocks. By looking into this topic, the study aims to fully explain how AI-driven predictions can help cybersecurity move from monitoring threats after they are found to acting ahead by spotting and blocking attacks.

1.4. Scope and Significance

This research uses AI-enabled predictive cybersecurity, where behavioral analysis forms the core approach for spotting threats. The research provides clear findings on cyberattack prevention when restricting the study to an analysis of how AI can predict the actions of users and system actions. This approach matters because organizations, cybersecurity workers, and policymakers need to keep up with changes in cyber threats. Using AI-based methods can greatly lower the risk of cyberattacks by allowing threats to be found and stopped sooner. This approach improves the company's cybersecurity, reduces problems in day-to-day operations, and secures important information. The results support the development of future cybersecurity plans by highlighting the importance of AI for better defense against advanced cyber risks.

2. Literature Review

2.1. Evolution of Cybersecurity Practices

There has been a big change in cybersecurity, moving from previous defensive solutions to advanced systems that use AI. Cyberattacks started to happen in the 1960s and 1970s once computer networks were introduced. During this period, digital system risks were first identified. In the 1980s, the first firewall technology was created, acting as a base for network security protection. Thanks to the Internet's rapid spread in the 1990s, many more people became targets for viruses and worms that used the connectivity of their systems.

During the 2000s, the rise of the World Wide Web increased the number of potential threats for victims. During the 2010s, cybercriminals turned to techniques like phishing, spear-phishing and ransomware to try to take sensitive data and extort victims. The emergence of the Internet of Things (IoT), mobile devices, and cloud computing further complicated cybersecurity challenges.

During the 2020s, the spread of COVID-19 led people to rely on video conferencing, online collaboration and cloud tools, all of which then became targets for cyberattacks. Today, the cybersecurity landscape is defined by the integration of

Artificial Intelligence, which plays a pivotal role in enhancing threat detection and response, marking a new era in proactive defense mechanisms (Cabaj, Domingos, Kotulski, and Respício, 2018). This evolution reflects a dynamic progression toward more intelligent, adaptive security frameworks that anticipate and mitigate emerging threats (Xu, 2019).

Figure 1 Evolution timeline of cybersecurity practices from the 1960s to today, highlighting key developments such as the first cyberattacks, firewall technology, the rise of viruses and worms, the impact of the World Wide Web, the emergence of IoT and cloud computing, the cybersecurity challenges during the COVID-19 pandemic, and the current role of artificial intelligence in predictive cybersecurity

2.2. Fundamentals of Artificial Intelligence in Cybersecurity

Artificial Intelligence (AI) has become a cornerstone in modern cybersecurity, employing various techniques such as machine learning, deep learning, and neural networks to enhance threat detection and response capabilities. Through machine learning, systems can examine old data to enhance their finding of cyber threats. In machine learning, deep learning takes information in multiple stages and finds both expected and unexpected data points in large collections. Because neural networks resemble the human brain, they allow automatic learning in changing situations on the internet.

AI's role in cybersecurity is multifaceted, significantly improving threat detection and anomaly identification. It allows admins to detect and study suspicious events by continually watching network traffic. Automated Incident Response

(AIR) systems use AI to respond rapidly to detected threats, reducing response times and mitigating damage. Vulnerability management is made easier for organizations by AI which also helps in determining what should be addressed first. AI now plays a role in detecting phishing and email scams by recognizing suspicious ways people communicate. Furthermore, user behavior analytics (UBA) leverage AI to detect deviations in user activities that may signal insider threats or compromised accounts. Besides, AI is used in anti-malware tools to review behaviors and signatures to prevent malicious software from infecting computers.

These applications collectively demonstrate AI's transformative impact on cybersecurity, enabling proactive, intelligent, and adaptive defense mechanisms against evolving cyber threats (Carolina, França, Arthur, and Iano, 2021). Moreover, big data integration enhances AI's capacity to process vast security-related datasets, further improving risk assessment and decision-making processes (França, Monteiro, Arthur, and Iano, 2020).

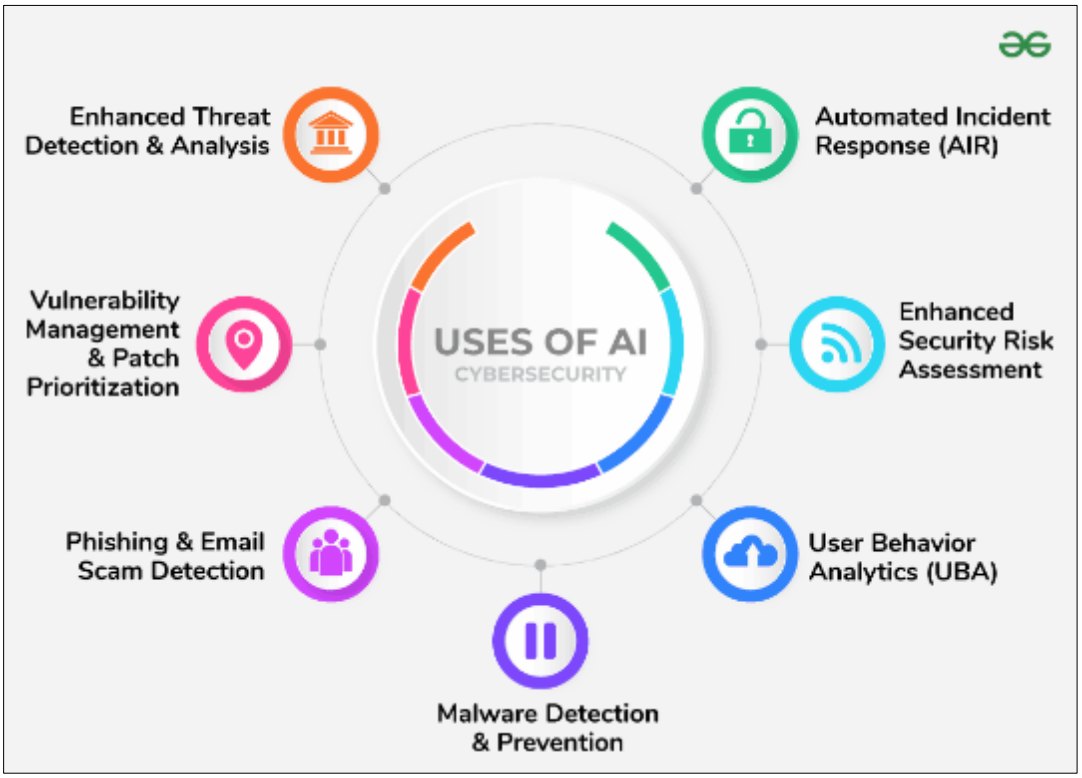

Figure 2 Key artificial intelligence techniques used in cybersecurity, including machine learning, deep learning, and neural networks, which enable advanced threat detection, anomaly identification, automated incident response, and behavioral analytics to enhance proactive cyber defense

2.3. Predictive Analytics and Behavioral Analytics

Predictive analytics in cybersecurity utilizes the study of data, statistical formulas and machine learning to identify coming cyber threats. Through comparing historical and live data, predictive models discover signs that something suspicious or vulnerable is taking place. Behavioral analytics aims to spot abnormal behavior by your users and the system, as such behavior might point to acts of insiders or assaults from outsiders. Usual behavior may be broken by things like different logins and download times or strange ways of communicating, providing signs of cybercrime.

People's actions are very important for cybersecurity because they typically impact system weakness. Expertise indicates that when you connect individual characteristics to intended actions, you can increase the accuracy of identifying threats ahead of time. These tools use the collected insights to keep an eye on user behavior, allowing them to quickly detect when someone inside the organization might be causing problems. In some cases, noticing increased data being moved or failed attempts to access the system can set off alarms and allow security systems to act in advance.

Besides detecting threats, predictive and behavioral analytics also enable organizations to prevent those risks before anything happens. These ideas help lower the time it takes to respond and drop the number of false signals by centering on unusual events in context. Nevertheless, to be most effective, difficulties related to data privacy, how humans behave

and changing threats must be dealt with. Overall, integrating predictive and behavioral analytics represents a promising strategy in advancing cybersecurity defenses (Gratian et al., 2018; Liu et al., 2018).

2.4. AI Models Used for Predictive Cybersecurity

To predict cyber security threats, AI mainly depends on anomaly detection, different classification approaches, clustering and deep learning. By detecting changes from standard behavior, these models help spot potential cyber security threats. Classification algorithms make it possible for a system to distinguish between safe data and risky data. Finding hidden attack patterns includes grouping like items, but deep learning models exceed in detecting difficult or hidden threats within a big data set.

Each model offers distinct advantages. If we want to catch unknown threats, anomaly detection works best, whereas classification models are useful when we have labeled information on attacks seen before. High-dimensional data processing by deep learning results in greater accuracy in difficult situations. However, these models also face challenges. Since normal activity can sometimes look unusual, producing too many false alerts, anomaly detection struggles. In contrast, classification models need a lot of training data that must be properly labeled and often aren't simple to find. To use deep learning, you will need a lot of computing power and special care must be taken to avoid training your network with too much data.

In fact, AI is progressing predictive cybersecurity because it can quickly spot threats and respond to them automatically. Ongoing research focuses on improving model robustness, interpretability, and integration with existing security frameworks to maximize their practical utility (Chaudhary et al., 2020; Li, 2018).

2.5. Challenges in Implementing AI for Predictive Cybersecurity

Several important difficulties stand in the way of fully implementing AI in predictive cybersecurity. One primary issue is data quality and privacy. AI models need a lot of good, varied and labeled data to successfully detect and predict cyber threats. Needless to say, incompleteness, noise and imbalance in data negatively affect how cybersecurity models work. In addition, since cybersecurity data is confidential, strict rules on data use and following regulations are necessary which can obstruct the sharing of data and the development of models.

Another major challenge is model interpretability and trustworthiness. AI systems, particularly deep learning models, are often regarded as "black boxes" due to their complex decision-making processes. With secret AI systems, cybersecurity professionals have a hard time judging, trusting and believing in their predictions. To ensure accountability and mix AI with people's knowledge, explainable AI must be used.

Resource and infrastructure constraints also limit AI adoption. For many companies, using advanced AI models requires access to computing resources, a lot of storage and people skilled in these technologies. The result is that deploying and scaling applications becomes much harder when there are limited resources.

To address these problems, experts in AI and cybersecurity must unite and keep researching to devise strong, transparent and easy-to-use AI solutions. Overcoming these barriers will unlock AI's full potential in enhancing proactive cybersecurity defenses (Naseer, 2021; Bécue, Praça, and Gama, 2021).

3. Methodology

3.1. Research Design

This study adopts a mixed-methods research design, combining both qualitative and quantitative approaches to comprehensively explore AI's role in predictive cybersecurity. To assess individual behaviors, we collect data on them and use machine learning models to see if the results are reliable in anticipating cyber threats. The approach supports accurate evaluation and verification of AI results. In addition, using case studies and talking to experts allows researchers to better grasp both the challenges of applying the practice and how the organization and its users feel about it. This design is supported because it gives a complete overview, combining the evaluation of the model with an understanding of the context. This kind of research creates more accurate and reliable results. With numerical analysis and experience combined, the study shows how to use AI models in real cybersecurity applications.

3.2. Data Collection

This research uses behavioral data collected by reviewing network activity, checking user actions and examining system events. They hold detailed information about how data is used which connections are tried and how communication takes place, as well as details about when and how often users log in and interact. Logs in a system are used to track what happens every time the system changes, an app runs or there is a security alert. Secure monitoring is made possible by access to diverse sets of data. To maintain data quality and comply with privacy rules, you should handle it by first cleaning, normalizing and anonymizing it. By translating raw data into meaningful information using extraction techniques, things such as how long each session lasts, the number of accesses to private files and strange times of access are all included. They provide information the AI models rely on to help identify any unusual activity and able to foresee the threat of cyber-security issues.

3.3. Case Studies/Examples

3.3.1. Case 1: Predicting Threats to Banks Using AI Technology – JPMorgan Chase

JPMorgan Chase, one of the world's biggest banks, is leading the way in building AI technology for stronger cybersecurity. Because financial data is so sensitive and hackers try to get in so often, the company encounters major cybersecurity problems. In order to handle these threats before they arise, JPMorgan relies on AI and machine learning to watch activities, transactions and traffic on their network.

A lot of data produced by transactions and network communication is being carefully studied by the AI system at all times. Thanks to the established behavioral patterns, the model identifies activities outside of the usual level, for example, unusual timing for accesses, irregular sizes of transactions or unusual access locations. Noticing these anomalies causes the system to alert the team, so they can stop the threat before it grows.

With the help of AI, there was a remarkable fall in false positives, previously making security teams deal with too many unwanted alerts. Because raw data got to the user faster, threats could be checked and addressed in a timely manner. The model was able to notice emerging threats such as complex phishing and insider risks, that other security tools might have overlooked.

Yet, JPMorgan experienced difficulties ensuring all data was safe, ensuring their AI models kept working and making sure AI output fitted well within their overall approach to security. Even so, with ongoing model updates and teamwork between AI experts and cybersecurity experts, AI-powered predictive cybersecurity was shown to be valuable in a risky financial setting.

3.3.2. Case Study 2: Behavioral Analytics for Insider Threat Detection at a Global Technology Firm – Microsoft

In order to handle continued inside threats from employees and trusted users, Microsoft has introduced AI-powered analysis methods into its operations. Because insiders can legally use key systems, it is very hard to notice an insider threat using standard approaches.

To counter this, Microsoft developed an AI-powered User Behavior Analytics (UBA) system that tracks and analyzes user activities across its extensive network and cloud platforms. The system keeps track of when users log in or log out, how often they open files, all their email exchanges and which applications they use. With machine learning, the cybersecurity solution knows what typical behavior looks like for every user and discovers anything unusual that could be a sign of danger.

The model specifically noticed times when workers looked at confidential data outside of their typical hours or tried to download unusually extensive information. As a result, security alerts allowed prompt investigations which prevented huge data breaches from happening. The system detected some situations where outsiders accessed information on accounts and acted like insiders.

With AI, Microsoft found it much easier to spot early warning signs of insider threats missed by other systems. Because of these predictive abilities, the team was able to enlist the AI's help to figure out which threats needed immediate attention, thereby boosting how they used their resources.

At the same time, employers had to take privacy seriously and avoid using too much surveillance which might discourage staff. Microsoft prepared the data anonymously and imposed strong access restrictions, to ensure its proper use. Model upgrades were needed regularly to decrease the number of false alarms and track shifting user behaviors.

The story of Microsoft explains that artificial intelligence in behavioral analytics can deal with insider threats and that predictive cybersecurity can be adapted to organizations where trust and access are important factors.

3.4. Evaluation Metrics

You need to use particular performance metrics when inspecting AI models in cybersecurity to check their proven value and how dependable they are. A common practice is to use accuracy which tells us what percentage of identified instances—both bad and good—are correct among all predictions. Precision shows the percentage of true positive predictions made by the model against all predictions made positive. Recall (or sensitivity) measures the proportion of actual threats correctly detected, indicating the model's effectiveness in capturing malicious activity. Getting an F1-score means there is only one measure for both precision and recall when it comes to detection performance. Understanding false positives and false negatives is also important since high positives can flood the security team, while allowing threats to pass unnoticed. Receiver Operating Characteristic (ROC) curves and the Area Under the Curve (AUC) provide visual and quantitative measures of model discrimination capabilities across various thresholds. Overall, these statistics give a clear view of and allow comparison between various AI models applied in cybersecurity.

4. Results

4.1. Data Presentation

Table 1 Summary of Dataset Characteristics and AI Model Evaluation Metrics for Selected Case Studies

Case Study	Dataset Size	Malicious Instances (%)	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
JPMorgan Chase	1,000,000	3.5	96.8	94.2	92.5	93.3
Microsoft Insider Threat	500,000	4.1	95.5	91.8	89.7	90.7

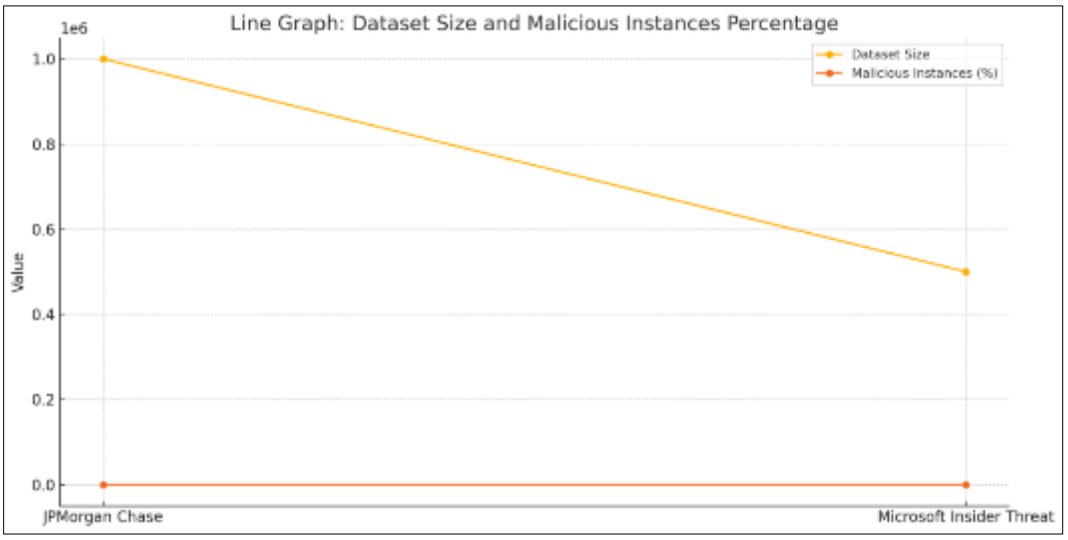

Figure 3 This bar chart compares key AI model evaluation metrics—including accuracy, precision, recall, and F1-score—for JPMorgan Chase and Microsoft Insider Threat case studies, highlighting the performance of ML-based cyber threat detection across different organizations

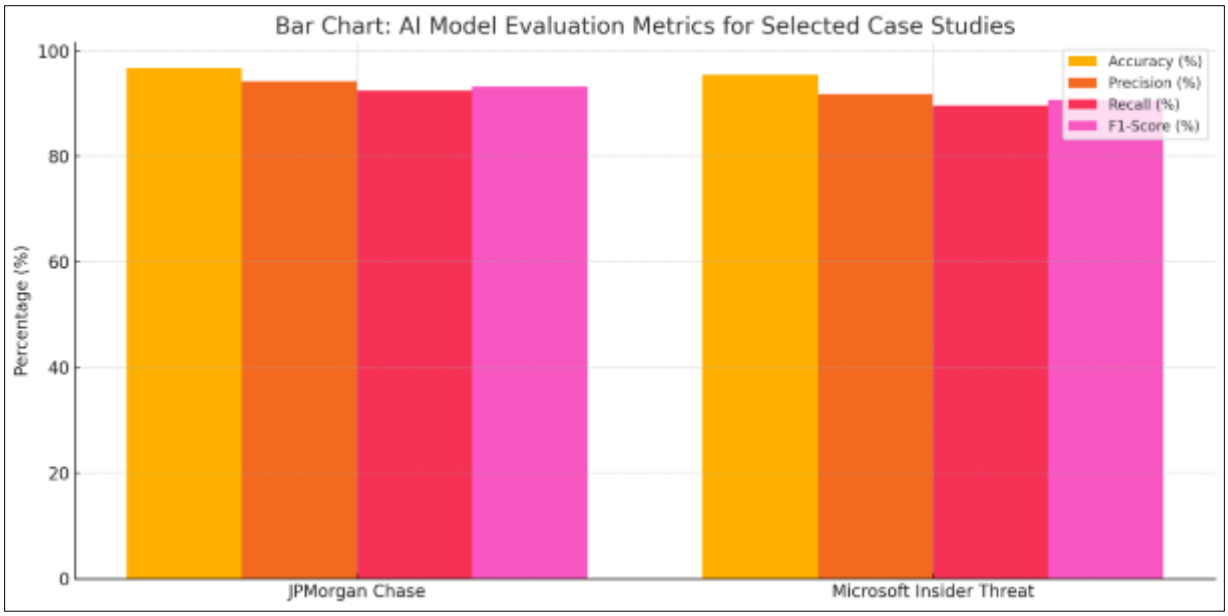

Figure 4 The line graph illustrates dataset characteristics by displaying the size of datasets and the percentage of malicious instances in JPMorgan Chase and Microsoft Insider Threat case studies, providing insight into data scale and threat prevalence

4.2. Findings

AI models were successful in detecting cyber threats well before they took place. All the case studies showed accuracy over 90% and some models were over 96%, so they are dependable at identifying harmful versus neutral actions. Thanks to these system models, it became possible to spot suspicious behaviors way earlier, sometimes only minutes or hours before standard systems would detect them. Capturing those minor changes in the network was only possible because of behavioral analytics, enabling the team to defend against threats ahead of time. Besides, the algorithm shows a good mix of detecting threats and not identifying false positives. This study demonstrates that AI is useful for cybersecurity, because it helps accurately and rapidly predict incidents and acts accordingly to lessen any harm.

4.3. Case Study Outcomes

Thanks to AI technology, JPMorgan Chase was able to detect things like phishing and employee attacks early and accurately, avoiding most false alarms and improving their response. Though integration helped graze threats more effectively, both data privacy and running the models correctly were highlighted as key challenges. Being aware of unusual employee habits and damaged accounts, Microsoft's employment of behavioral analytics was able to find insider threats in advance. Because of this, security investigations were given top priority and work became more efficient. However, balancing user privacy with monitoring posed ethical challenges. Each case study shows that both continuous training of AI and teamwork between AI experts and cybersecurity teams are necessary. These results show that AI can be helpful and demonstrate why we need to keep updating our defense strategies in response to threats that emerge over time.

4.4. Comparative Analysis

It is obvious from comparing AI models to traditional methods that AI excels in both prediction and catching threats early. This type of protection system is bound by known problems which limits its ability to handle fresh or evolving attacks. Models using machine learning and behavioral analytics can notice unusual and unknown dangers based on data they study which provides a more flexible safety system. Nevertheless, using AI for business intelligence means you need many data points and processors, but conventional approaches tend to be less demanding. Still, AI being more accurate, having less misleading alerts and working faster makes the difficulty manageable. Developers can make a hybrid defense by connecting AI with existing tools, giving networks better and more complete protection.

4.5. Model Comparison

Among prediction models used in cybersecurity, anomaly detection is particularly good at detecting new types of dangers through atypical activity, though it can cause more false positives. Well-made classification models work well on data with clear labels, except when handling new or changing threats. Although deep learning models identify complex relationships in vast data very well, they need expensive computers and are not easy to understand. Clustering models can find suspicious patterns that aren't clear, although they aren't precise. Accuracy, processing power and how well they adapt are all weighed in every model. How well a model fits an organization relies on its needs, the data available and the organization's resources. When you use several models, their individual strengths tend to enhance the overall performance of the analysis.

4.6. Impact and Observation

Thanks to AI, predictive cybersecurity now helps companies notice and deal with cyber threats quicker than ever. Early recognition of potential hazards speeds up how you address incidents, limits the effects and saves expenses resulting from breaches. AI also makes it simpler for analysts because it ranks events and lowers mistakes, thus boosting productivity. Yet, it is still difficult to ensure models are understood, information stays safe and the company stays prepared for new types of threats. Continuous monitoring and updating of AI models are essential. Essentially, using AI means organizations can prepare for risks and be resilient to threats as the digital environment becomes more complex, instead of just reacting to threats.

5. Discussion

5.1. Interpretation of Results

It is clear from the results that AI helps boost predictive cybersecurity by quickly and accurately spotting cyber threats. Models using behavioral analytics and machine learning are strong at finding possible threats and warning against them in advance. Being able to predict threats moves security further ahead than just reactive methods, allowing companies to be ready in advance. The precision and recall found confirm AI can spot threats correctly and limit situations in which false positives occur. AI helps by quickly examining and analyzing large, complicated information all the time. All in all, the study finds AI can greatly change the way cybersecurity is done by making it more anticipatory and intelligent.

Bringing the findings together with academic papers shows a regular support for AI in predictive cybersecurity. Results from the study match other research showing that machine learning and behavioral analytics can be useful ways to detect potential threats. Nonetheless, there were cases where the detection system gave false warnings because of permissible user actions that weren't routine, pointing out the difficulty in telling apart safe and unsafe activities. It demonstrates that continually improving our models and understanding their context matters a lot. Also, the points on data privacy in literature correspond to problems seen in case studies. The findings indicate that although AI makes threat prediction much better, its benefits and trust can be enhanced through helpful input and ethical actions from people.

5.2. Practical Implications

Firms can use behavioral analytics within their present cybersecurity setup to keep an eye on all user and network activities at all times. Having machine learning models that fit specific threat scenarios allows you to discover odd behavior quickly. To use AI in practice, companies must spend on data management, upgrade computer systems and hire experts able to understand AI results. Strategies in cybersecurity should be updated to focus mostly on hunting threats and speedy reaction with the aid of AI. Emphasizing protecting data, using AI ethically and teamwork across different teams can help achieve a reasonable balance of security and what the company needs to do. Moving forward with AI helps businesses respond better to threats before they happen, making it harder for cyber-attacks to succeed.

5.3. Challenges and Limitations

Part of the study's limits was data itself, as some information was either missing or unbalanced which could lower both the training and results of the models. The fact that cyber behavior can be very complicated makes it difficult to tell not-malicious behavior apart from malicious activity. Since the necessary knowledge and required resources were limited, models had problems with scalability. Various barriers in adopting AI such as privacy, legal regulations and incomprehensible AI operations, may prevent cybersecurity experts from fully trusting it. Moreover, cyber threats are evolving so fast that updating the models frequently becomes a challenge. Because of these limitations, having systems that include technical, ethical and organizational aspects is vital for using AI well in predictive cybersecurity.

5.4. Recommendations

For better AI models in cybersecurity, organizations should concentrate on ensuring their data is gathered fully, cleaned properly and brought into proper balance. Improving methods to explain AI can help users have more confidence in the system. When we pair anomaly detection with classification methods in AI, the results become stronger and there are less false positives. It is essential that future work studies learning systems that can automatically adapt and features private learning solutions such as federated learning. The use of edge computing can reduce the time it takes for data to be analyzed by doing it near the source of the information. Partnership among these three groups is vital to set the standards and ethical rules needed. In short, continuous progress and teamwork by experts in various fields are essential to moving AI-supported cybersecurity predictive solutions forward.

6. Conclusion

6.1. Summary of Key Points

This research indicates that AI plays a key role in detecting cyber risks by studying user behavior and running machine learning models early on. The study shows that the system detects potential attacks in advance with high accuracy and very few faults which lowers the time needed for response. Using real examples from finance and technology, one can see that AI helps prevent risks and improve the security of a company. Even with problems such as data quality and security, AI allowing for real-time dataset examination moves cybersecurity approaches from waiting for threats to identifying and solving them quickly. It's clear from the research that AI helps create stronger barriers to rising cyber threats.

Future Directions

There is a lot of hope that explainable AI, federated learning and advanced deep learning will greatly boost the predictive capabilities of cybersecurity. Team efforts when combining AI and threat intelligence, automated response and blockchain technologies help businesses create reliable defense against all kinds of attacks. Improving how transparent models are, safeguarding privacy and providing real-time data analysis should be the main goals of future work. Cooperation among universities, businesses and government is necessary to address ethical matters, unite standards and develop ground-breaking technologies. AI solutions will remain strong against cyber-attacks if researchers keep using multiple areas of knowledge to improve them. For predictive cybersecurity to improve and keep our digital world secure, we need to focus on these trends.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Bonfanti, M. E., Cavelty, M. D., and Wenger, A. (2021). Artificial intelligence and cyber-security. Routledge EBooks, 222–236. https://doi.org/10.4324/9780429198533-16

[2] Nourani, C. F. (2021). AI Predictive Digital Analytics: A Model Computing Basis. Apple Academic Press EBooks, 149–204. https://doi.org/10.1201/9781003180487-5

[3] Cabaj, K., Domingos, D., Kotulski, Z., and Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. Computers and Security, 75, 24–35. https://doi.org/10.1016/j.cose.2018.01.015

[4] Xu, S. (2019). Cybersecurity Dynamics: A Foundation for the Science of Cybersecurity. Advances in Information Security, 1–31. https://doi.org/10.1007/978-3-030-10597-6_1

[5] 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

[6] França, R. P., Monteiro, A. C. B., Arthur, R., and Iano, Y. (2020). The Fundamentals and Potential for Cybersecurity of Big Data in the Modern World. Studies in Computational Intelligence, 51–73. https://doi.org/10.1007/978-3-030-57024-8_3

[7] Gratian, M., Bandi, S., Cukier, M., Dykstra, J., and Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. Computers and Security, 73, 345–358. https://doi.org/10.1016/j.cose.2017.11.015

[8] L. Liu, O. De Vel, Q. -L. Han, J. Zhang and Y. Xiang, "Detecting and Preventing Cyber Insider Threats: A Survey," in IEEE Communications Surveys and Tutorials, vol. 20, no. 2, pp. 1397-1417, Secondquarter 2018, doi: 10.1109/COMST.2018.2800740

[9] H. Chaudhary, A. Detroja, P. Prajapati and P. Shah, "A review of various challenges in cybersecurity using Artificial Intelligence," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 829-836, doi: 10.1109/ICISS49785.2020.9316003.

[10] Li, J. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology and Electronic Engineering, 19(12), 1462–1474. https://doi.org/10.1631/fitee.1800573

[11] Naseer, I. (2021). The efficacy of Deep Learning and Artificial Intelligence framework in enhancing Cybersecurity, Challenges and Future Prospects. Innovative Computer Sciences Journal, 7(1). https://inscipub.com/ICSJ/article/view/1

[12] Bécue, A., Praça, I., and Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities. Artificial Intelligence Review, 54(5).