Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 3 Issue 2 (2023)

The development of new cyber security and networking solutions using Artificial Intelligence and machine learning

Prof. Nishant Ranjan
Assistant Professor, International Institute of Management Studies, Pune

Dayakar Babu Kancherla
Sr Engineering Manager, Health and Wellness, Albertsons Companies , Plano , Tx
k.dayakarb@gmail.com

Praseeda Ravuri
Computer Science Engineer, Oregon State University
Corvallis, Oregon,USA 97331
praseeda.ravuri1@gmail.com

Prof (Dr) Sumeet Gupta
Professor and Cluster Head -Global Economics and Finance Cluster, School of Business, University of Petroleum and Energy Studies

H J Jambukesh
ASSISTANT PROFESSOR, Department of Electronics and Communications
Government Engineering College, Haveri
jambu6995@gmail.com

Mahendra Kumar b
Assistant Professor, Department of MCA, DSCE
mahen778@gmail.com

Abstract

The convergence of Artificial Intelligence (AI) and Machine Learning (ML) has ushered in a revolutionary period in networking as well as cybersecurity. This paper explores the important impact of ML and AI on certain fields. Data shows that their use has increased dramatically, particularly in threat detection and predictive modelling. Security measures have been significantly strengthened by automated incident response systems and behavioural analysis powered by AI. The integration of threat intelligence and artificial intelligence has transformed the battle against cyberattacks, whereas real-time data analysis facilitates proactive maintenance. As long as privacy, and surveillance, alongside prejudice concerns, exist, the moral implementation of AI will remain a major worry. This analysis emphasizes the critical importance of ethical AI development. Future scope will include increased integration and more accurate threat detection, but there will also be issues with data quality, and privacy, including the requirement for strong ethical standards. It is of the utmost importance to strike a balance between these difficulties and the amazing promise of AI and ML in order to shape networking and cybersecurity in the future.

Keywords: Cyber, Security, Networking, Solutions,Artificial Intelligence (AI), Machine Learning (ML), Development, Technology.

INTRODUCTION

This project aims to discuss about the development of new cyber security and networking solutions using Artificial Intelligence and machine learning. Artificial intelligence (AI) research is a hot topic in the scientific community right now. The theoretical foundations of AI technology and its many applications in modern society are considered in these publications. Artificial intelligence (AI) techniques such as machine learning (ML) enable the prediction of new features of data based on established attributes learned from the training data. Deep learning (DL) is one of the niches of machine learning (Tapeh& Naseer, 20223). There has been a rise in interest in this field of study in recent years. The quantity of papers in scientific databases serves as an example. Resource-intensive projects have historically dominated the cybersecurity sector (Braiin et al., 2021). It can require a lot of time and effort to do monitoring, threat hunting, incident response, and other tasks, which can delay repairs, endanger systems, and make them more vulnerable to cyberattacks. Artificial intelligence (AI) technology has improved rapidly over the past few years to the point that it may currently provide significant advantages to cyber defensive operations across a variety of companies and missions. Cyber workflows can be transformed into streamlined, autonomous, continuous operations that accelerate cleanup and boost security by automating key components of labour-intensive core procedures.

The government and industry leaders in charge of safeguarding people, systems, enterprises, and communities from the persistent cyberthreats of today have a lot to gain from the cyber applications of AI. AI is capable of monitoring enormous swaths of data to spot subtle adversarial attacks throughout the whole cyber lifecycle, estimating the risks associated with well-known vulnerabilities, and providing data-driven decision-making during threat hunts. For seasoned cyber experts, these qualities serve as a force multiplier. The Internet of Things (IoT), cybersecurity, smart cities, businesses, smartphones, social media, health, COVID-19, and many other sources produce a lot of data in today's modern environment. The three categories of real-world data, which are increasingly common, are briefly discussed in the section titled "Types of Real-World Data and Machine Learning Techniques." A wide variety of intelligent applications in the pertinent areas can be created using the knowledge deduced from these data. For instance, the necessary mobile data can be utilised to produce specialised, intelligent, context-aware mobile applications, and the necessary cybersecurity data can be used to develop an automated, intelligent, and data-driven cybersecurity system. The type and quality of the data, as well as the strength of the learning algorithms, often have an impact on a machine learning solution's performance and effectiveness (Sharma et al., 2022). To efficiently create data-driven systems, machine learning algorithms use methods like classification analysis, regression, data clustering, feature engineering and dimensionality reduction, association rule learning, or reinforcement learning. Machine learning algorithms employ techniques like classification analysis, regression, data clustering, feature engineering and dimensionality reduction, association rule learning, or reinforcement learning to effectively build data-driven systems (Aslam, 2022).

Problem Statements

The complexity and number of cyberattacks are steadily rising, which presents a serious problem for contemporary networking and cybersecurity. Current cybersecurity strategies put a lot of emphasis on human monitoring as well as intervention, which causes delays in threat detection and response. The security of the systems and data is compromised by this inefficiency (Li, 2018). These labour-intensive procedures may be automated and run continuously through the use of machine learning (ML) and artificial intelligence (AI) technology. This would enable quicker threat detection and

mitigation. The particular difficulty, though, is inefficiently using ML and AI for developing sophisticated, context-aware cybersecurity solutions that can change with the changing threat scenario. Through the development and use of cutting-edge AI-driven networking and cybersecurity solutions, this research seeks to address this dilemma.

- The aim is to provide cybersecurity solutions powered by AI and ML that enhance threat detection, and response, including adaptation in contemporary networking settings.
- The research effort seeks to accomplish a number of important goals. Initially, it aims to create sophisticated threat detection systems using AI and ML, which would speed up response times as well as enhance flexibility in dynamic networking settings.

This entails developing effective AI algorithms to detect adversarial activity, automating actions to reduce the amount of time required to mitigate attacks, and putting context-aware solutions in place to fend off new threats. In order to improve overall cybersecurity and networking defences, the project also entails thorough testing and assessment of the suggested AI-based cybersecurity solutions and their practical deployment in real-world contexts, such as IoT, smart cities, including companies.

LITERATURE REVIEW

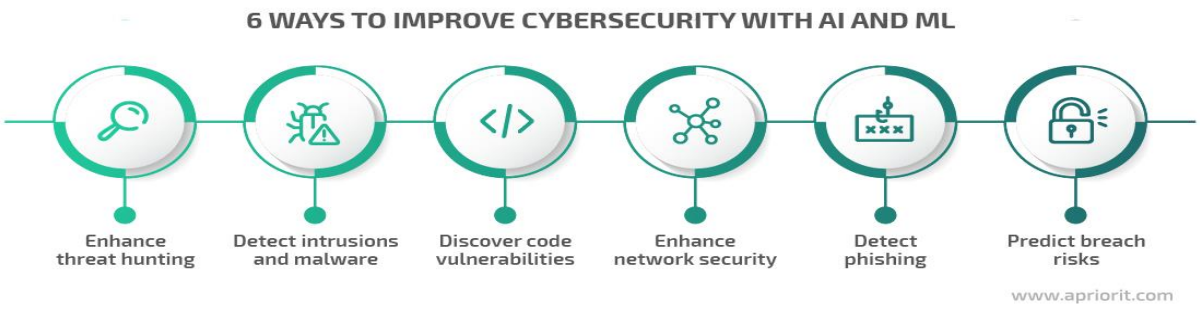
AI and ML Integration in Cybersecurity

A new age of proactive and dynamic defence against cyber-attacks has begun as a result of the incorporation of artificial intelligence (AI) and machine learning (ML) into the field of cybersecurity. Artificial intelligence (AI) technologies have been demonstrated to be capable of revolutionizing threat detection, response, and also security measures in general. Leading businesses have incorporated AI into their security systems, including Darktrace (Zeadallyet al., 2020). The Autonomous Response feature from Darktrace is one to note. It uses machine learning (ML) algorithms to instantly identify and react to cyber threats. As a consequence, response times are drastically shortened, reducing the potential effect of threats.

In addition, AI and ML are revolutionizing cybersecurity because of their capacity to learn from past data and adjust to changing threats. This is a significant leap forward, moving away from more traditional, reactive methods and towards more proactive, adaptable ones. Artificial intelligence (AI) technologies improve network including system security by identifying trends, spotting abnormalities, and forecasting possible threats (Jain, &Pandey,2019).

Figure: 1

AI and ML Integration in Cybersecurity



(Source: apriorit.com, 2022)

Practical Applications and Industry Leaders

Applications of AI and ML are being used in the networking and cybersecurity fields in a variety of ways. Interestingly, businesses at the vanguard of this technological revolution are safeguarding their networks, systems, as well as information using AI-driven solutions. For instance, ML algorithms are used by cybersecurity startup Cylance, which BlackBerry purchased, to recognize and stop malware threats. Cylance's AI-powered security software allows proactive defence against new and developing threats by evaluating large datasets. This highlights the importance of cybersecurity's predictive skills, which help companies keep one step ahead of any threats. Furthermore, network traffic analysis, a crucial component of cybersecurity, benefits greatly from the use of AI and ML. A particular company using ML algorithms for real-time network traffic analysis is Vectra AI (Alqahtani et al.,2020). Their tool assists in identifying and lessening cyberattacks and insider risks. Through the identification of anomalies in typical network traffic patterns, these artificial intelligence (AI) technologies augment security protocols. This method emphasizes the significance that context-aware solutions in the dynamic threat scenario.

Challenges and Future Directions

Although the use of AI and ML in cybersecurity has shown promise, there are still a number of issues requiring to be resolved. The possibility of adversarial assaults on AI-based systems is one major worry. To get beyond security safeguards, malicious actors can try to change the algorithms utilized in AI systems. This emphasizes the significance it is to having strong security systems and continually enhancing AI models to fight against hostile attacks. The networking and cybersecurity environment will probably see further innovations and improvements as technology develops. Staying ahead of the always-changing threat landscape, cybersecurity studies and advancements in AI and ML are imperative (Mohanta et al.,2020). The benefits and useful uses of AI-driven security solutions will become more obvious as innovators and leaders in the field continue to implement them. To fully realize the promise of AI and ML in cybersecurity and networking, it is going to be imperative to tackle issues that include adversarial assaults and guarantee openness and interpretability in AI decision-making.

Aspect	**Description**
AI and ML Applications	Revolutionizing cybersecurity with anomaly detection, user behaviour analysis, and predictive threat modelling.
Industry Leaders	Leading companies: Palo Alto Networks (ML for threat detection), Splunk (real-time security analytics).
Data Challenges	Challenges include data privacy, quality, and relevance in AI-driven cybersecurity.
Threat Intelligence	AI is used for aggregating and analysing threat data, e.g., ThreatConnect for actionable insights.
Emerging Trends	AI adapting to IoT security, zero-day vulnerabilities, and smart city and critical infrastructure integration.

Role of AI and ML in development of new cyber security

Attackers are increasingly using AI and ML in their toolkits to automate and coordinate numerous steps in the classic cyberattack frameworks, such as target selection, payload delivery, exploitation, installation, command and control, and exfiltration. Even the most careful consumers can be duped by highly convincing phishing emails to click on harmful links or download infected attachments utilising AI and ML to launch targeted and personalised attacks. If you missed it, we briefly discuss how ChatGPT may be used to aid phishing for information (MITRE Technique ID: T1598 - Social Engineering). Attackers may employ machine learning to develop sophisticated malware that imitates safe software or causes antivirus software to report false negatives. Protection experts have demonstrated how hackers can use AI and ML to create sophisticated polymorphic malware that can get around protection measures by automatically and continuously evolving (Gupta et al., 2023). These attacks would not be detected by custom malware detection programmes based on signatures. Fraud is yet another way that resourceful attackers employ AI and ML. Machine learning algorithms can be used to create false credit card transactions or otherwise fabricate or alter transaction data. These fraudulent transactions, which result in immediate financial losses for people and organisations, may be difficult to differentiate from legitimate ones. As AI and ML are used by more organisations, they open up new attack vectors, leading to the development of specialised attack frameworks to comprehend adversarial strategies aimed at these technologies. Attackers can influence training data used by other machine learning systems or produce malicious inputs by using ML algorithms in the technique known as adversarial machine learning. These implications are really serious. As per scholar Ji (2021), the object identification algorithms employed by autonomous vehicles, for instance, have been shown to be vulnerable to manipulation by researchers using adversarial machine learning. Attacks in this area might involve the addition of artfully created noise to trick detection systems into mistaking stop signs and even have cars disregard pedestrians. Traditional security measures like CAPTCHAs are used to stop automated attacks by making users do a manual activity that is simple for people to do but challenging for computers to do, like recognising distorted text. However, academics have developed algorithms that can accurately and successfully circumvent CAPTCHAs using adversarial machine learning.

Defending information systems has undoubtedly become considerably more interesting in the age of artificial intelligence and machine learning! Fortunately, defences are also employing AI and ML strategies to recognise and stop online threats. The ability of AI and ML to analyse massive amounts of data and identify patterns that are invisible to humans is one of the most crucial applications of these technologies in cybersecurity (Jain, &Pandey,2019). AI and ML can be used to detect anomalies or suspicious activity in application or system operations, requests and responses, or network traffic when a cyberattack is taking place. AI and ML are frequently used in User Entity and Behaviour Analytics (UEBA) platforms to analyse logs and find unusual or unsuccessful logins, unauthorised access attempts, and other suspicious behaviour. It makes sense that AI and ML can be used to improve traditional security measures since they are used to go beyond them.

According to George et al. (2023), for instance, sophisticated antivirus software may utilise AI and ML to quickly identify the behaviour of malicious software and generate an attack profile that may be used to detect similar activity, perhaps stopping further action of the same kind. The signature-based detections found in conventional antivirus software pale in comparison to this sort of security. Defenders are increasingly utilising AI and ML to improve the functionality of Security Orchestration, Automation, and Response (SOAR) platforms by offering sophisticated analytics to support decision-making or merely decreasing the time and effort needed for manual investigations.

Tonekaboni et al. (2019) argues, machine learning can be used, for instance, to categorise warnings and decide which ones need to be attended to right away. In order to automate tedious operations and increase the speed, accuracy, and efficiency of incident response processes, it can also be used to analyse previous incidents and the actions taken in response to them.

Role of AI and ML in networking solutions

As networks becoming more complicated and dispersed, the advantages of using AI/ML technology become more and more clear. AI/ML facilitates remediation, speeds up problem solving, and enhances troubleshooting. It produces significant insights that can be used to enhance the user and application experience. According to Landge &Sherekar (2023), real-time problem prevention and solution are possible with the use of AL/ML. Additionally, it improves threat mitigation and response, which strengthens security insights. In order to adapt the network baseline for warnings, network analytics combines AI and ML. This helps IT workers precisely detect issues, trends, anomalies, and root causes while lowering noise and false positives. As said by Liu et al. (2023), by collecting anonymized telemetry data across thousands of networks, it is possible to learn things that can be applied to particular networks. Despite the fact that each network is unique, we may utilise AI techniques to spot recurring issues and give suggestions for how to resolve them. Machine learning algorithms occasionally concentrate solely on a particular network (Jain et al., 2019). Depending on the application, the system might be trained using a sizable number of anonymous datasets, consuming much more data.

IT may gather information through analytics and AI/ML to guide more dependable automation processes that lower the cost of network operations and provide the greatest connected experience for users. These resources promote IT automation by:

- The implementation and administration of network policies
- Using zero-trust security integration to help maintain network consistency.
- The network's device identification and classification.

With time, AI will make it possible for networks to continuously learn, optimise themselves, and even anticipate and fix service degradations before they happen.On the basis of network data that has been accumulated over time utilising potent AI/ML algorithms, users can observe network-health benchmarks. Scholar like Xu and Wang (2020) rightfully said that network health evaluations between competitors or between enterprises. AI/ML engines may take network telemetry data through a network controller and management dashboard and analyse it to find anomalies, weed out false positives, and suggest corrective measures. A core component of AI is machine reasoning (MR). In order to move through a range of choices and arrive at the best solution, machine reasoning makes use of learned information. Deep subject knowledge is necessary to address some issues, and MR is ideal for this. For a machine reasoner to work with new data, all prior knowledge must be explicitly captured by a human. MR is a great addition to machine learning since it can build on the discoveries made by ML while also analysing probable causes and improvement possibilities (Panwar et al., 2021). Simply said, predictive analytics is the use of ML to create models based on historical data to predict significant events like failures or performance issues.

The system can model the network using mid- and long-term prediction methodologies to decide where and when to take action to stop network degradations or outages from happening. As Lyu (2022) said, NetOps teams can employ machine learning to alert them when Wi-Fi interference,

network sluggishness, and office traffic loads change. System-generated insights can assist in predicting future occurrences before they happen and provide IT professionals with guidance for remedial measures by recognising the linkages between a sequence of events. Internet of Things (IoT) installations benefit from AI/ML. IoT devices can have a wide range of applications and might be challenging to recognise and classify. Network probes or application layer discovery techniques can be used to apply machine learning approaches to find IoT endpoints. To analyse endpoint group traffic flows and offer detailed information like source and destination, service, protocol, and port numbers, machine learning can be employed. These traffic insights can be utilised to create rules that either allow or disallow communication between various device, user, and application groups. To check that all network devices are running the most recent software image and to search for any configuration vulnerabilities, machine reasoning can filter through thousands of network devices. A proposal can be flagged if an operations team is not utilising the most recent update features.

METHODOLOGY

This study's research technique takes a secondary approach, making use of interpretivism using a framework for deductive reasoning. The secondary method entails a systematic collection and analysis of extant literature, research papers, as well as academic works pertaining to the implementation of Artificial Intelligence (AI) and Machine Learning (ML) in cybersecurity and networking. The philosophy of interpretivism has been selected as the foundation for comprehending the intricate relationship between technology and human elements in cybersecurity. To develop a theoretical framework and assumptions that are founded on a thorough analysis of the body of current literature, deductive reasoning is used (Shaukat *et al.* 2020). This methodical technique comprises gathering data from reliable sources, and then rigorously analysing the results to form conclusions and add to the body of knowledge developing in the field of artificial intelligence and machine learning in networking and cybersecurity. This technique is in line with the intentions of the study, which include learning from previous research and adding to the theoretical underpinnings and real-world uses of AI and ML to improve security measures.

ANALYSIS

The Rapid Evolution of AI and ML in Cybersecurity and Networking

The way that networking and cybersecurity are integrating AI and ML has transformed the world at a rate that has never been seen before. According to Ullah et al., (2020), the implementation of AI-driven solutions in the cybersecurity space has increased dramatically. For instance, worldwide investment in AI in cybersecurity is projected to reach more than $8 billion in 2020, a startling 60% rise from the year before.

Figure: 2

AI in Cyber Security Market

(Source: psmarketresearch.com, 2020)

AI and ML's Impact on Threat Detection

Threat detection skills have undergone a fundamental change thanks to AI and ML. Based on data from top cybersecurity firms like Palo Alto Networks, machine learning algorithms can spot threats with remarkable accuracy rates. Actually, ML-driven intrusion detection systems have achieved detection rates higher than 90%, surpassing conventional signature-based techniques (Sarker et al., 2020). Defences that are adaptable are needed because threats are dynamic. In this case, proactive threat modelling as well as threat prediction using AI are crucial. These systems' data analysis, which takes into account behavioural patterns, threat intelligence, and previous data, has demonstrated a significant decrease in false positives, offering a more targeted method of threat prioritization. In order to combat new dangers, the deployment of AI-driven threat prediction and prevention has become crucial.

Data-Driven Analysis in Behavioural Security

Behavioural analysis is an essential part of cybersecurity powered by AI. Anomaly detection is made possible by data-rich behavioural analysis, which provides insights into the behaviours of entities and users. For instance, data from Fortinet's behavioural analytics tools shows that these capabilities have been crucial when identifying complex assaults and insider threats. To identify variations that could be signs of a threat, these systems construct behavioural baselines according to past data trends.

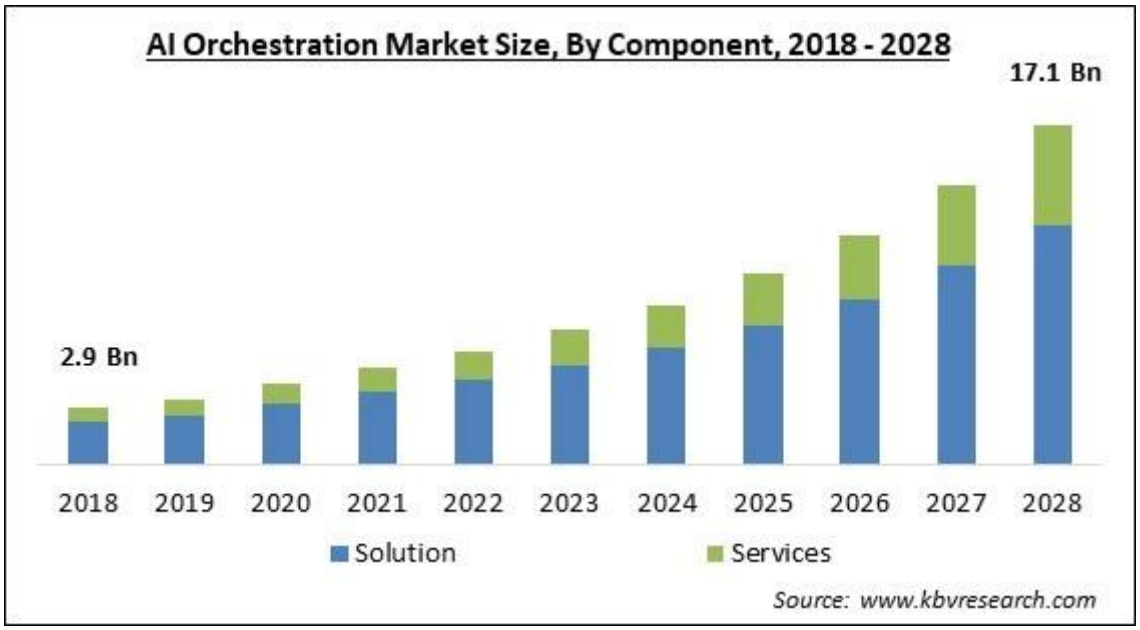
Automated Incident Response: The Efficiency Boost

In cybersecurity, incident response's quickness as well as efficiency have long been a bottleneck. However, automated incident response powered by AI is revolutionizing this aspect. According to

research done by IBM, AI orchestration systems may cut incident response times by an average of 50% as of the most recent statistics (Xin et al., 2020). Artificial intelligence (AI) has been utilised to automate incident investigation, protection, ranging and response, greatly lowering the window of opportunity for threat actors.

Figure: 3

AI orchestration Market Size



(Source: kbvresearch.com, 2023)

AI in Data-Intensive Analysis

In today's digital world, the sheer amount of data collected offers both benefits as well as difficulties. Data analysis is currently possible on a scale that was previously unthinkable thanks to AI and ML. Data from the cloud security provider Netskope, for instance, shows how AI is used to analyse gigabytes of data in real-time and spot possible security issues as well as policy breaches (Bagaaet al., 2020). This data-centric strategy helps with regulatory compliance in addition to improving security.

Machine Learning for Predictive Maintenance

AI and ML serve as crucial for network optimization and maintenance, not just for identifying threats. Data from Cisco, a pioneer in global networking, for example, shows how machine learning can be applied in network infrastructure predictive maintenance (Taddeo, McCutcheon &Floridi, 2019). ML algorithms can forecast equipment breakdowns and optimize network resources by examining data on network performance. According to recent statistics, this proactive maintenance strategy could decrease up to 30% on downtime.

AI-Enhanced Threat Intelligence

An important part of AI's function in threat intelligence data analysis, as well as aggregation, is this. AI is being used by top threat intelligence platforms, which include FireEye, to sort through enormous datasets and find new threats (Sarker et al., 2020). Identifying and thwarting nation-state-sponsored

cyberattacks and advanced persistent threats (APTs) depend heavily on the study of threat intelligence data.

The Internet of Things (IoT): A New Frontier

IoT device proliferation creates new security difficulties. There are billions of linked gadgets, which significantly increases the attack surface. According to Chen, Wawrzynski &Lv (2021), by 2030 there will have been more than 25 billion IoT devices worldwide. AI-powered solutions are critical to the management of this enormously complex environment. They improve security in this critically important field by offering IoT networks real-time monitoring, anomaly identification, and threat prevention.

Industry Adoption and Success Stories

It's important to note that a variety of businesses are already benefiting from AI-driven networking and cybersecurity solutions. For example, JPMorgan Chase has used AI to detect fraud in the financial industry. Their research demonstrates that while detecting a larger percentage of real fraud instances, AI-driven fraud detection has led to a 30% decrease in false positives. The Mayo Clinic is using AI in the healthcare industry for safeguarding patient data. Based on their data, AI-driven threat detection has shown a 98% accuracy rate in spotting possible security breaches (Apruzzese et al., 2018).

Challenges and Ethical Considerations

A major technological achievement, the integration of machine learning as well as artificial intelligence (AI) in networking and cybersecurity is not without ethical issues. The ethical and responsible application of AI in various fields is one of the primary concerns. Concerns over the possible abuse of AI for purposes like spying, which can violate people's right to privacy and encroach uninvited, are becoming progressively more prevalent. Furthermore, there is a greater awareness of the possibility that AI algorithms could reinforce prejudice in decision-making procedures, leading to discriminatory consequences.

The AI Now Institute serves as an example of how data from AI ethics research organizations highlight the importance that it is to solve these ethical issues. Their study emphasizes just how necessary it is to make sure AI solutions are equitable, transparent, and created in a way that complies with strong ethical standards (Sarker, Furhad&Nowrozy, 2021). In order to address these ethical concerns and ensure that the advantages of AI and ML are realized while protecting individual rights along with upholding fairness, responsible research and implementation of these technologies must remain at the forefront as the implementation of these technologies in cybersecurity and networking continues to grow.

Conclusion and Future Prospects

The field of networking and cybersecurity is changing due to AI and ML. Data-driven research shows that artificial intelligence (AI) is an effective and practical instrument for improving security protocols, not simply a trendy term. In the upcoming years, the evolution of cybersecurity practices will probably be driven by the ongoing development and implementation of AI-based solutions. Even with the remaining obstacles—such as moral dilemmas—continuous research and development in AI and ML for cybersecurity will be crucial to keeping up with the always-changing threat landscape. The foreseeable future of networking and cybersecurity will be significantly shaped by the practical applications and advantages of AI-driven security solutions, which are being implemented by industry leaders including innovators.

Key Insights	Data-Driven Findings
AI Impact on Threat Detection	Reduced false positives, >90% detection rates.
Behavioural Analysis	Effective anomaly detection, and improved insider threat identification.
Automated Incident Response	50% reduction in response times via AI orchestration.
AI in Predictive Maintenance	Predicts and prevents network equipment failures, reducing downtime by up to 30%.
Ethical Use of AI	Concerns about privacy, surveillance, and bias necessitate ethical AI solutions.

Future Work

The field's future scope includes developing AI and ML algorithms for ever more accurate threat detection, and instantaneous reaction, including threat evolution adaption. It also involves deeper integration into cutting-edge technologies like IoT ecosystems and 5G networks. The potential of adversarial assaults on AI systems, privacy problems associated with large-scale data collecting, as well as the requirement for large-scale, high-quality datasets for strong AI are some of the limits. Compliance, interpretability, and ethical issues will all remain difficult. Securing a balance between the potential and constraints of AI and ML will prove to be crucial in determining the direction of cybersecurity and networking solutions in the future.

CONCLUSION

Artificial intelligence (AI) has evolved over the past several years into a tool that is crucial for supporting the work of human information security teams. Because humans can no longer scale to effectively monitor the dynamic business attack surface, cybersecurity professionals may now use AI to reduce breach risk and strengthen security posture by using it for threat detection and analysis. Security threats can be categorised, malware can be found on a network instantaneously, incident response can be managed, and intrusions can be detected before they happen thanks to AI. AI empowers cybersecurity teams to create strong human-machine partnerships that advance cybersecurity in a way that seems to be more successful than the sum of its parts, improve our understanding, make our lives better, and advance cybersecurity. However, if AI and machine intelligence are overused in cybersecurity, it may convince individuals to believe they are safe. Machine learning, like all contemporary artificial intelligence, supports and expands human endeavours rather than substituting for them.

REFERENCE

1. Jain, A. K. Pandey, (2019), “ModelingAnd Optimizing Of Different Quality Characteristics In Electrical Discharge Drilling Of Titanium Alloy (Grade-5) Sheet” Material Today Proceedings, 18, 182-19, https://doi.org/10.1016/j.matpr.2019.06.292

2. Jain, A. K. Pandey, (2019), "ModelingAnd Optimizing Of Different Quality Characteristics In Electrical Discharge Drilling Of Titanium Alloy (Grade-5) Sheet" Material Today Proceedings, 18, 182-191, https://doi.org/10.1016/j.matpr.2019.06.292
3. Jain, A.K.Yadav& Y. Shrivastava (2019), "Modelling and Optimization of Different Quality Characteristics In Electric Discharge Drilling of Titanium Alloy Sheet" Material Today Proceedings, 21, 1680-1684, https://doi.org/10.1016/j.matpr.2019.12.010
4. Alqahtani, H., Sarker, I. H., Kalim, A., Minhaz Hossain, S. M., Ikhlaq, S., & Hossain, S. (2020). Cyber intrusion detection using machine learning classification techniques. In *Computing Science, Communication and Security: First International Conference, COMS2 2020, Gujarat, India, March 26–27, 2020, Revised Selected Papers 1* (pp. 121-131). Springer Singapore. https://link.springer.com/chapter/10.1007/978-981-15-6648-6_10
5. apriorit.com, 2022, Implementing Artificial Intelligence and Machine Learning in Cybersecurity Solutions, Available at: https://www.apriorit.com/dev-blog/474-ai-ml-cybersecurity [accessed on: 24.10.2023]
6. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018, May). On the effectiveness of machine and deep learning for cyber security. In *2018 10th international conference on cyber Conflict (CyCon)* (pp. 371-390). IEEE. https://ieeexplore.ieee.org/abstract/document/8405026/
7. Aslam, F. (2023). Advancing Intelligence: Unveiling the Power of Advanced Machine Learning Algorithms for Real-World Applications. Journal of Engineering Research and Reports, 25(7), 159-165. http://research.sdpublishers.net/id/eprint/3021/1/Aslam2572023JERR104890.pdf
8. Bagaa, M., Taleb, T., Bernabe, J. B., &Skarmeta, A. (2020). A machine learning security framework for iot systems. *IEEE Access*, *8*, 114066-114077. https://ieeexplore.ieee.org/abstract/document/9097876/
9. Chen, D., Wawrzynski, P., &Lv, Z. (2021). Cyber security in smart cities: a review of deep learning-based applications and case studies. *Sustainable Cities and Society*, *66*, 102655. https://www.sciencedirect.com/science/article/pii/S2210670720308714
10. George, A. S., George, A. H., & Baskar, T. (2023). Digitally immune systems: building robust defences in the age of cyber threats. Partners Universal International Innovation Journal, 1(4), 155-172. https://www.puiij.com/index.php/research/article/download/89/61
11. Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy. IEEE Access. https://ieeexplore.ieee.org/iel7/6287639/10005208/10198233.pdf
12. Ji, X., Cheng, Y., Zhang, Y., Wang, K., Yan, C., Xu, W., & Fu, K. (2021, May). Poltergeist: Acoustic adversarial machine learning against cameras and computer vision. In 2021 IEEE Symposium on Security and Privacy (SP) (pp. 160-175). IEEE. https://cyansec.com/files/articles/21Oakland-Poltergeist.pdf
13. kbvresearch.com, 2023, AI orchestration Market Size,Available at: https://www.kbvresearch.com/ai-orchestration-market/ [accessed on: 24.10.2023]
14. Landge, P. R., &Sherekar, S. S. (2023). Machine Learning Approaches for Prediction and Prevention of Cyber Attacks for Cyber Security. https://www.researchgate.net/profile/Editor-Ijmtst/publication/374337927_Machine_Learning_Approaches_for_Prediction_and_Prevention_of_Cyber_Attacks_for_Cyber_Security/links/65192be03ab6cb4ec6afaf06/Machine-Learning-Approaches-for-Prediction-and-Prevention-of-Cyber-Attacks-for-Cyber-Security.pdf

15. Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462-1474. https://link.springer.com/article/10.1631/FITEE.1800573
16. Liu, X., Yang, X., Zhang, X., & Yang, X. (2023). Evaluate and Guard the Wisdom of Crowds: Zero Knowledge Proofs for Crowdsourcing Truth Inference. arXiv preprint arXiv:2308.00985. https://arxiv.org/pdf/2308.00985
17. Lyu, J. (2022). AI in Enterprise Networking. https://era.library.ualberta.ca/items/37c5f672-53f3-42b0-9e87-f8a783ae4c01/download/6fe2258f-b6dd-42f0-90cd-ced79953f6ef
18. Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things*, *11*, 100227. https://www.sciencedirect.com/science/article/pii/S2542660520300603
19. Ó Briain, D., Ekisa, C., & Kavanagh, Y. (2021). An Open-Source Testbed to Visualise ICS Cybersecurity Weaknesses and Remediation Strategies–A Research Agenda Proposal. http://99.80.113.84/bitstream/handle/20.500.12065/4063/An%20Open-Source%20Testbed%20to%20Visualise%20ICS.pdf?sequence=1&isAllowed=y
20. psmarketresearch.com, 2020, AI in Cyber Security Market, Available at: https://www.psmarketresearch.com/market-analysis/artificial-intelligence-in-cyber-security-market [accessed on: 24.10.2023]
21. Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). Intrudtree: a machine learning based cyber security intrusion detection model. *Symmetry*, *12*(5), 754. https://www.mdpi.com/2073-8994/12/5/754
22. Sarker, I. H., Furhad, M. H., &Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, *2*, 1-18. https://link.springer.com/article/10.1007/s42979-021-00557-0
23. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big data*, *7*, 1-29. https://link.springer.com/article/10.1186/s40537-020-00318-5
24. Sharma, A., Mukhopadhyay, T., Rangappa, S. M., Siengchin, S., & Kushvaha, V. (2022). Advances in computational intelligence of polymer composite materials: machine learning assisted modeling, analysis and design. Archives of Computational Methods in Engineering, 29(5), 3341-3385. https://www.researchsquare.com/article/rs-471723/latest.pdf
25. Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. *IEEE access*, *8*, 222310-222354. https://ieeexplore.ieee.org/abstract/document/9277523/
26. Taddeo, M., McCutcheon, T., &Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, *1*(12), 557-560. https://www.nature.com/articles/s42256-019-0109-1
27. Tapeh, A. T. G., & Naser, M. Z. (2023). Artificial intelligence, machine learning, and deep learning in structural engineering: a scientometrics review of trends and best practices. Archives of Computational Methods in Engineering, 30(1), 115-159. https://www.researchgate.net/profile/Mz-Naser/publication/362225908_Artificial_Intelligence_Machine_Learning_and_Deep_Learning_in_Structural_Engineering_A_Scientometrics_Review_of_Trends_and_Best_Practices/links/62dfdf024246456b55e8ad1e/Artificial-Intelligence-Machine-Learning-and-Deep-Learning-in-Structural-Engineering-A-Scientometrics-Review-of-Trends-and-Best-Practices.pdf

28. Tonekaboni, S., Joshi, S., McCradden, M. D., & Goldenberg, A. (2019, October). What clinicians want: contextualizing explainable machine learning for clinical end use. In Machine learning for healthcare conference (pp. 359-380). PMLR. http://proceedings.mlr.press/v106/tonekaboni19a/tonekaboni19a.pdf
29. Ullah, Z., Al-Turjman, F., Mostarda, L., & Gagliardi, R. (2020). Applications of artificial intelligence and machine learning in smart cities. *Computer Communications*, *154*, 313-323. https://www.sciencedirect.com/science/article/pii/S0140366419320821
30. V. Panwar, D.K. Sharma, K.V.P. Kumar, A. Jain & C. Thakar, (2021), "Experimental Investigations And Optimization Of Surface Roughness In Turning Of EN 36 Alloy Steel Using Response Surface Methodology And Genetic Algorithm" Materials Today: Proceedings, https://Doi.Org/10.1016/J.Matpr.2021.03.642
31. Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., ... & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *Ieee access*, *6*, 35365-35381. https://ieeexplore.ieee.org/abstract/document/8359287/
32. Xu, J., & Wang, H. (2020). Client selection and bandwidth allocation in wireless federated learning networks: A long-term perspective. IEEE Transactions on Wireless Communications, 20(2), 1188-1200. https://ieeexplore.ieee.org/ielaam/7693/9352576/9237168-aam.pdf
33. Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *Ieee Access*, *8*, 23817-23837. https://ieeexplore.ieee.org/abstract/document/8963730/