The Future of Cyber Defence: Predictive Security with Artificial Intelligence

Goutham Kacheru
Senior Engineer, Department of Information Systems Technologies
Wilmington University, New Castle, Delaware, USA 19720.

Abstract:

The increase in the complexity and number of cyber threats has made the old reactive security systems not enough to handle the present situation. Because of this, predictive cybersecurity is coming as a proactive method that is using old attack records, behaviour study and advanced analytics to guess the threat before it happens. The main part of this change is the use of Artificial Intelligence, especially machine learning models that can find abnormal activities, connect the threat signs and give real-time alerts. This article is explaining how AI is supporting predictive security using supervised and unsupervised learning methods, anomaly detection and automation in threat intelligence. Even though this method is giving good results like faster threat detection, less false alerts and better visibility in hybrid setups, still there are some problems. The issues related to data quality, attacks to fool the AI, need for human control and following the ethics rules are still important. This paper finally dwells about the new trends like federated learning and threat data sharing using blockchain which will play a role in building future AI based self working cybersecurity systems.

Keywords: Predictive Cybersecurity, Artificial Intelligence (AI), Machine Learning, Threat Intelligence Anomaly Detection.

I. INTRODUCTION

In the present digital period, where all the modern systems are depending on information technology, cybersecurity is becoming an important matter for governments, industries and common people. The size of attack possibility is growing very fast due to the usage of cloud computing, mobile based platforms, IoT devices and remote working style. At the same time, the attackers are also becoming more advanced by using methods like APTs, changing types of malware, supply chain based attacks and even AI based attack models. Because of this situation where there is more vulnerability and smarter attackers, the old type reactive security systems which are working only after an attack are now showing their limits.

In earlier days, the cybersecurity method was mostly dependent on fixed rule-based systems like firewalls, signature based antivirus and IDS[1]. These systems were useful for already known threats but they are not good when the attack is new or changing very quickly like zero-day attacks or malware that is hiding its behaviour. These reactive tools are also making the response slow and this delay can cause more damage, loss of data or disturbance in services. In the current fast-moving threat world, where even seconds are important to control the situation, there is a serious need for a forward-looking and predictive type of defense system[2]-[4].

This changing threat environment has led to the development of predictive cybersecurity which is a new type of approach that is focusing on stopping the threats before they fully happen. The

main part of predictive cybersecurity is Artificial Intelligence, mainly machine learning which is a group of algorithms that can find patterns, detect abnormal activities and keep changing based on new data[5]. By studying large amounts of past data, behaviour logs and threat signs, AI systems can understand possible risks and give timely alerts so that organisations can stay ahead of the attackers.

Different from the traditional systems, the predictive models are not only depending on fixed rules or already known attack types[6]-[10]. These models are using supervised, unsupervised and reinforcement learning methods to find hidden connections and behaviour changes in the live data. This is useful for finding insider threats, beginning stages of ransomware, side movement of attackers inside the network and also new zero-day attacks. When this AI is combined with threat intelligence like global threat data, open source intelligence and indicators of compromise, it is improving the understanding and is converting the raw data into useful information that can be used for action.

The main aim of this paper is to study the changing role of AI in building the future of cyber defense using predictive analytics[11]. It is discussing how AI based models are changing the cybersecurity work by helping in faster threat detection, reducing the wrong alerts and increasing the visibility of threats in complicated systems[12],[13]-[15]. This paper is also covering the real time usage examples, important technologies, connection with threat intelligence and the actual advantages of using predictive methods. It is also looking into problems like bias, attacker based manipulations, data related issues and ethical points to give a clear view of both the benefits and risks of AI based security.

At the end of this paper, the readers will be able to fully understand how predictive cybersecurity which is supported by AI is changing the way of defense and making the organisations ready to handle future cyber threats with strength and planning.

II. What is Predictive Cybersecurity?

Predictive cybersecurity is a method that is using advanced data analytics and artificial intelligence to find, understand and reduce the cyber threats before the attack actually happens. The main features of this method are early threat detection, non-stop monitoring of data and the ability to learn and change according to new types of attacks[16]. It is different from the traditional security methods which are depending on fixed rules or already known threat signs. Predictive systems are using probability based models and pattern finding techniques to guess the possible risks.

Old security tools like signature-based antivirus or rule-based intrusion detection systems (IDS) are working in a reactive way. They need to know about the attack in advance and are not able to catch zero-day attacks or new attacking styles[17]. But predictive cybersecurity is using machine learning methods which are able to learn from past attack data and find the hidden signs of threats.

The success of predictive systems is based on their power to handle and study huge amounts of mixed data from different sources. This includes:

- Past attack data which is useful to find repeating threat types and plans.

- User and device behaviour which is helping to find the unusual activities that are not matching with the normal pattern.
- System and network logs which are giving detailed information about the working, data movement and possible signs of attack.

The main focus of predictive cybersecurity is on real-time checking, which is helping the organisations to act quickly when early danger signs are seen. By learning continuously and matching the different data types, these systems are giving a future focused security setup that is reducing the time needed to respond and increasing the understanding of the current situation.

III. Role of Artificial Intelligence in Predictive Security

Artificial Intelligence is acting like the main analysis engine behind predictive cybersecurity because it is helping to find patterns automatically and detect unusual behaviour in real time from complex data systems[18]. The AI methods are good in catching small hidden connections and changes which can show some kind of attack even if those patterns are not known before or not marked. This kind of feature is very important for stopping cyber attacks before they happen, especially in systems which are big or always changing.

In the centre of AI's role is machine learning which is a part of AI that helps systems to study from old data and keep getting better with time. Different types of machine learning are used in cybersecurity such as supervised, unsupervised and reinforcement learning.

- Supervised learning is using data that is already marked with known attacks and normal actions. These models are good in identifying already known threats and giving alerts when similar things happen again. Some common methods are decision trees, support vector machines and neural networks.
- Unsupervised learning is working without marked data and is useful to find abnormal activities or unusual behaviours. Methods like k-means, DBSCAN for grouping and PCA for reducing dimensions are used to catch activities that are different from the normal ones. These differences can show some new or unknown threats.
- Reinforcement learning is not used very commonly but it is helpful in changing environments where AI is learning how to defend by doing trial and error. These models can change their working according to new attack situations and can help in preventing intrusions and setting smart rules.

Using these models, AI systems are able to detect the strange user activities like login at unusual times, accessing the data without permission, or doing movement inside the network which are not normal. Also the possible zero-day attacks can be identified by checking the behaviour of code activities which look like an attack but are different from the usual patterns. Malicious network actions like command and control communication or the stealing of data also can be detected before the main attack is executed. So AI is helping cybersecurity to become preventive and not only reacting to the already known attacks but also predicting and stopping the new type of risks. When AI is included in the cybersecurity activities, the

traditional fixed systems are changing into smart and learning based systems which can work quickly and also on a large scale.

IV. Predictive Analytics in Action

Many cybersecurity solutions have shown the real time usage of predictive analytics which is proving that AI can be used for stopping the threats before they cause any damage[19]. These real industry cases are showing how machine learning and behaviour checking are used to predict and control the attacks even before it affects the operations.

(i) Early Ransomware Detection – Darktrace

Darktrace which started in 2013 and was first to use unsupervised machine learning to find threats inside the company networks. Its Enterprise Immune System model was studying the normal behaviour of users and devices to find any early sign of attack[20]. In case of ransomware, Darktrace was able to catch the file encryption and unusual data movement before the encryption is finished so that early action can be taken. Its live threat display and automatic response features were considered useful for reducing the time needed to control the attack.

(ii) Insider Threat Detection – CrowdStrike Falcon

CrowdStrike Falcon was using a cloud based architecture with machine learning that was built inside to understand the user behaviour and find insider threats. It was checking the access style, how credentials are used and the sideways movement inside the network to guess the harmful intention without depending on signature based methods[21]. One important feature was its threat graph which was collecting live data from many endpoints and was supporting predictive analytics on a large scale. Because of this, organisations were able to detect and check suspicious actions even before the data is stolen or access rights are misused.

(iii) Predictive Threat Alerts – Microsoft Defender ATP

Microsoft Defender Advanced Threat Protection, which was later renamed as Microsoft Defender for Endpoint, was also using behaviour sensors and cloud analysis to give predictive warning messages[22]. It was using supervised learning to detect the attack styles which are matching with MITRE ATT&CK framework and was helping the security team to get early alerts for sideways movement, wrong use of access power and continuous attack presence. It was also connected with threat intelligence sources to match attack signs across many companies which helped in giving trusted predictions about upcoming threats.

V. Integrating AI with Threat Intelligence

Threat intelligence is the process of collecting, studying and sharing the data that is related to current and future cyber attacks. It includes both technical details like malware hash values, IP addresses, domain names and also the background details like the attacker methods, techniques and plans[23]. Before it was mostly used for knowing the situation and responding after the attack. But now with AI it is becoming a tool that can be used before the attack happens. When AI is combined with threat intelligence it is improving the usage by making the analysis automatic, reducing the human effort and helping to take quick actions. This combination is

working through the handling of threat feeds, Open-Source Intelligence (OSINT), Indicators of Compromise (IOCs).

1) Threat feeds: AI systems are collecting live data from global security sources, company alerts and industry based reports. These feeds are having compromise signs which AI can quickly match with the internal system data.
2) OSINT: AI is using NLP and entity finding methods to take useful attack related information from public forums, security related blogs, pastebins and even dark web sites. It is helping to turn the unstructured data into usable form to give early information about attack plans or new vulnerabilities.
3) IOCs: AI and machine learning are used to check how serious the IOC is inside the company setup and to decide whether it is a real threat or just a harmless sign. AI also connects these IOCs to attackers, campaigns or known malware types.

Enhanced threat intelligence is providing some advanced features which are made possible through AI support such as automated correlation and triaging: AI systems are matching the internal warning messages with the global threat intelligence sources so that the unwanted alerts are removed and only the important alerts are kept. It is also helping to arrange the alerts based on how serious and urgent they are.

AI is giving a risk score to each threat by checking how easily it can be used, how open the system is, and how much it can affect the business. The extra context is helping the analysts to know not only what has happened but also why it is important. By continuously learning from past incident results and feedback, AI is giving useful suggestions which are on time and matching with the security goals. These include fixing steps, searching queries and activity patterns to watch for. So the combination of AI and threat intelligence is changing the method from just collecting threat data to a smart and changing type of defense. By turning the threat details into early warning signals, AI is helping to build a cybersecurity system that can predict and prevent better.

VI. Benefits of Predictive AI-Based Cybersecurity

The combining of predictive analytics and artificial intelligence into the cybersecurity systems has given visible benefits mainly in detection time, correctness and better use of resources. These benefits are very important especially now when many organisations are moving towards hybrid, cloud and remote based systems which are increasing the number and difficulty level of security related events.

(i) Faster Detection and Response

AI based systems are supporting live monitoring and fast analysis of different types of data which is helping to bring down the average time to detect (MTTD) and average time to respond (MTTR). The machine learning models are always learning from the changing threat behaviours so they can guess the harmful activities and give alerts or take automatic actions in

just a few seconds. This fast action is very important to stop big attacks like ransomware, data stealing or wrong access level increase.

(ii) Reduction in False Positives

Normal security tools are giving too many alerts, many of which are false, and this is making the analysts miss the real threats. Predictive AI models are reducing this problem by using probability methods and smart filtering based on context to remove the normal harmless changes. Methods like ensemble learning and feedback based tuning are helping to increase the correctness slowly, so the security team can give more attention to the alerts that are serious and important.

(iii) Better Resource Allocation in SOCs

Security Operations Centers (SOCs) are also facing problems like less number of staff and more people leaving the job. AI is helping here by doing the regular checking work automatically, so the skilled people can be used for harder tasks like deep investigation and threat searching[24]. Dashboards and smart response steps based on AI are giving better understanding of the current threat and helping the SOC teams to take quick and clear actions based on their level.

(iv) Enhanced Threat Visibility in Hybrid, Cloud, and Remote Environments

Now the company network is spread over in-house systems, cloud, mobile devices and outside networks. Predictive AI is improving the view of all these areas together by joining the data, finding connections between platforms and giving the full picture of risk in one place[25]. This is very important in setups where the old type of border based protection is not useful or not possible.

So overall, predictive AI based cybersecurity is improving the work efficiency and the ability to handle threats, and it is giving scalable support for the growing and fast changing threat situations of today.

VII. Challenges and Limitations

Even though predictive AI based cybersecurity is getting used more and more, still there are many important problems that are affecting its trust, scaling and fair usage. These issues are showing that it needs to be used carefully with regular checking and support from experts in different fields.

(i) Data-Related Issues: Quality, Availability, and Representativeness

Predictive models are depending a lot on good quality and mixed data to correctly find the threats. But in real cases, the security data is usually broken, noisy or not complete because of different ways of logging or not enough access to threat related information. One more problem

is that many AI models are trained with old data which may not fully match the new or changing types of attacks. This is making the prediction less correct. If the dataset is small or narrow, the AI may miss many attacks, especially new ones like zero-day threats or those coming from specific areas.

(ii) Risk of Bias in Training Datasets

Also the training data can have hidden bias based on the place or organisation. For example, if one type of user or attack is shown more in the data, the AI may start giving more focus to that and ignore the other types[26]. This can lead to wrong alerts like calling a normal user as an attacker or missing some new trick used by a hacker. If the data is not selected and checked properly, the AI models may keep or even increase these biases which will reduce the trust of the system.

(iii) Adversarial AI: Evasion and Poisoning Attacks

AI systems are facing the problem of being attacked by adversarial methods. In an evasion attack, the attacker is making small changes in the input so that it behaves in a different way and the system will not detect it. For example, hiding malware in such a way that it will not be identified. In a poisoning attack, the attacker is giving wrong training data to the model so that it will slowly change the behaviour. These types of threats are affecting the correctness of AI based security and there is a need for strong checking and model protection methods.

(iv) Dependence on Skilled Human Analysts

Even though AI is doing automatic detection and sorting, there is still a need for human monitoring. Analysts are needed for checking the alerts, finding the root cause and also making changes in model results[27]. So using AI properly in cybersecurity depends on the people who have knowledge in both cybersecurity work and data science. But there is a lack of such skilled persons and it is becoming a challenge for full scale usage.

(v) Ethical and Privacy Considerations in User Behavior Monitoring

Predictive security is also requiring the full time checking of user actions, system usage and network data. But this type of checking is creating privacy concerns about data control, user permission and who is owning the data[28],[29]. If not handled carefully, AI systems can break the user rights or go against privacy rules. So ethical usage requires clear working, less data exposure and following legal policies like GDPR which was already active.

These problems are showing the need for using AI with balance with proper rules, human checking and regular update systems so that the cybersecurity can work in a responsible and trusted manner.

VIII. Future Outlook

As cyber threats are becoming larger and more advanced, the direction of predictive cybersecurity is now being influenced by new developments like decentralized learning, secure data systems and automation. When artificial intelligence is combined with these upcoming technologies, it is giving hope for stronger and more flexible security systems, but at the same time it is also bringing new legal and ethical issues.

(i) Trends Shaping the Future

a) Federated Learning

Federated learning is one method where the machine learning models are trained using data from different places without collecting the actual raw data in one place. It is showing good potential in cybersecurity because it is helping different organisations to work together and improve the threat detection models while keeping their sensitive data private. This method is useful in areas like healthcare and finance where data privacy rules are very strict.

(b) AI + Blockchain for Secure Data Sharing

The combination of AI with blockchain is also coming up as a secure way to share threat intelligence. Blockchain has features like unchangeable data and decentralised systems which are making the threat information more trustable and trackable. AI can then use this data to analyse and match the threats across different organisations. This method is helping to solve the old problem of trust and dependability in sharing threat data between different groups.

(c) Autonomous Cybersecurity Systems

In future, cybersecurity solutions are expected to move towards self-healing and self-defending types of architectures. These systems will be working independently using reinforcement learning and continuous behaviour analysis which can change itself according to new attack methods without any human support. These systems will try to find, react and recover from cyber problems in near real time, and move towards complete automatic cyber protection systems.

(ii) Anticipated Regulatory Frameworks

As predictive AI systems are becoming more useful in the real world, the checking from regulatory bodies will also increase. There are discussions going on for having control systems to make sure the AI decisions are fair, clear and responsible. Laws like GDPR in the EU have already pointed out the issue between using the data and protecting privacy. In future, it is expected that there will be clear rules for explainable AI, audit checking and reducing the data used in AI based security.

(iii) Ethical AI Development in Cyber Defence

Ethical thinking will become very important in predictive cybersecurity. There will be questions about how fair the AI is, what side effects it can create, and what rights the users have when they are being watched. So the AI systems should be made with support from different groups and must focus on human monitoring, proper responsibility, no unfair

judgement in attack detection and clear information about the monitoring and how the AI is working.

So overall, the development of predictive cybersecurity will depend not only on the new technologies but also on how well it is matching with the public needs, legal laws and ethical thinking. Using privacy based AI methods and proper management will be very important for gaining trust and long-term working.

IX. Conclusion

The movement from reactive type of cybersecurity to predictive cybersecurity is showing a basic level change in the way organisations are handling the changing digital threats. AI powered systems mainly using machine learning are helping in early prediction of threats by studying the old patterns and also finding the behaviour changes at the same time. These kinds of technologies are already showing their usefulness in improving the detection speed, reducing the false alerts and helping the security operations in more complicated environments. But for the proper working of these systems, responsible usage is very important which includes handling the problems like correctness of data, attacks that are trying to confuse the AI system and also the ethical related problems. As the attackers are also starting to use AI, it is very important that the defenders also improve their predictive systems by giving proper investment and applying the governance methods. In the coming time, AI will not just help the cybersecurity but it will become the main part of how cybersecurity will work.

REFERENCES

[1] I. A. Mohammed, “How artificial intelligence is changing cyber security landscape and preventing cyber attacks: a systematic review,” vol. 4, no. 2, pp. 659–663, Jun. 2016.

[2] R. Palthya, “AI-based Systems Enhance Cybersecurity Defenses, Identify and Mitigate Cyber Threats in Real-Time,” *International journal of science and research*, vol. 10, no. 8, pp. 1290–1295, Aug. 2021.

[3] S. Mohanty and S. Vyas, “Cybersecurity and AI,” Apress, Berkeley, CA, 2018, pp. 143–153.

[4] M. Yildirim, “Artificial Intelligence-Based Solutions for Cyber Security Problems,” IGI Global, 2021, pp. 68–86.

[5] A. Dalal, “Cybersecurity And Artificial Intelligence: How AI Is Being Used in Cybersecurity To Improve Detection And Response To Cyber Threats,” Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 9, no. 3, pp. 1416–1423, Dec. 2018.

[6] J. Fnu, “Emerging Threats: The Latest Cybersecurity Risks and the Role of Artificial Intelligence in Enhancing Cybersecurity Defenses,” International Journal of scientific research and management, Feb. 2021.

[7] F. Tao, M. S. Akhtar, and J. Zhang, “The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey,” EAI Endorsed Transactions on Creative Technologies, vol. 8, no. 28, p. 170285, Jul. 2021.

[8] K. Morovat and B. Panda, “A Survey of Artificial Intelligence in Cybersecurity,” International Conference on Computational Science, pp. 109–115, Dec. 2020.

[9] M. S. Malik, “Role of Artificial Intelligence in Cybersecurity Improvement,” International journal for electronic crime investigation, vol. 5, no. 1, pp. 43–51, Aug. 2021.

[10] B. Geluvaraj, P. M. Satwik, and T. A. A. Kumar, "The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace," Springer, Singapore, 2019, pp. 739–747.

[11] A. M. S. N. Amarasinghe, W. A. C. H. Wijesinghe, D. L. A. Nirmana, A. Jayakody, and A. M. S. Priyankara, "AI Based Cyber Threats and Vulnerability Detection, Prevention and Prediction System," Dec. 2019.

[12] D. Bogatinov, M. Bogdanoski, and S. Angelevski, "AI-Based Cyber Defense for More Secure Cyberspace," IGI Global, 2017, pp. 1471–1489.

[13] N. Kaloudi and J. Li, "The AI-Based Cyber Threat Landscape: A Survey," ACM Computing Surveys, vol. 53, no. 1, pp. 1–34, Feb. 2020.

[14] I. H. Sarker, I. H. Sarker, H. Furhad, and R. Nowrozy, "AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions," vol. 2, no. 3, pp. 1–18, Jan. 2021.

[15] K. Hasan, S. Shetty, and S. Ullah, "Artificial Intelligence Empowered Cyber Threat Detection and Protection for Power Utilities," Color Imaging Conference, pp. 354–359, Dec. 2019.

[16] E. Tyugu, "Artificial intelligence in cyber defense," International Conference on Cyber Conflict, pp. 1–11, Jun. 2011.

[17] Z. Zhang et al., "Artificial intelligence in cyber security: research advances, challenges, and opportunities," Artificial Intelligence Review, pp. 1–25, Mar. 2021.

[18] X. Feng, Y. Feng, and E. S. Dawam, "Artificial Intelligence Cyber Security Strategy," Dependable Autonomic and Secure Computing, pp. 328–333, Nov. 2020.

[19] R. Trifonov, S. Manolov, R. Yoshinov, G. Tsochev, and G. Pavlova, "Artificial Intelligence Methods for Cyber Threats Intelligence," vol. 02, Aug. 2017.

[20] S. B. Atiku, A. U. Aaron, G. K. Job, F. Shittu, and I. Z. Yakubu, "Survey On The Applications Of Artificial Intelligence In Cyber Security," International Journal of Scientific & Technology Research, vol. 9, no. 10, pp. 165–170, Oct. 2020.

[21] B. Naik, A. Mehta, H. Yagnik, and M. Shah, "The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review," Complex & Intelligent Systems, pp. 1–18, Aug. 2021.

[22] N. N. Abbas, T. Ahmed, S. H. U. Shah, M. N. Omar, and H. W. Park, "Investigating the applications of artificial intelligence in cyber security," Scientometrics, vol. 121, no. 2, pp. 1189–1211, Sep. 2019.

[23] P. T. Ezwenilethu, "Cybersecurity artificial intelligence system," Nov. 29, 2018.

[24] S. Zeadally, E. Adi, and Z. Baig, "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity," IEEE Access, vol. 8, pp. 23817–23837.

[25] T. O. Bazalgette, D. M. Humphrey, and C. J. Salji, "Artificial intelligence (ai) based cyber threat analyst to support a cyber security appliance," Nov. 12, 2020.

[26] S. S. Vaddi, C. S. Koganti, S. K. Kalyana, and P. Anudeep, "Artificial Intelligence Based Predictive Threat Hunting In The Field of Cyber Security," Oct. 2021.

[27] R. Morla, "Ten AI Stepping Stones for Cybersecurity," arXiv: Cryptography and Security, Dec. 2019.

[28] S. K. Adabala, "Machine Learning in Cybersecurity: Proactive Threat Detection and Response," International Journal For Multidisciplinary Research, vol. 3, no. 5, Sep. 2021.