International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 12 Issue 7 ǁ July 2024 ǁ PP. 203-213

Using Machine Learning to Achieve Cyber Security Requirements: A Comprehensive Review of Thwarting cyber-attacks in real time

M. Alsalamony[1],
[1]*Department of Information Systems, Faculty of Computers and Artificial Intelligence, Fayoum, Egypt*

Abstract: *The modern cyber security landscape requires innovative solutions to keep pace with the ever-changing landscape of cyber threats. There has been a paradigm shift toward the integration of artificial intelligence (AI) and machine learning (ML) due to the tremendous hurdles facing traditional methodologies. While applying artificial intelligent techniques to address computer security challenges is not a novel concept, the machine learning algorithms have recently garnered significant interest within the computer security community. Machine learning (ML) plays a crucial role in enhancing cyber security by meeting various requirements essential for protecting systems, networks, and data from malicious attacks. This paper carefully examines how AI and ML can strengthen real-time cyber security, focusing on quickly predicting and stopping cyber-attacks. It drives the investigation into using advanced technologies to enhance cyber security. The shortcomings of traditional methods highlight the need to explore how effective AI & ML can be in enhancing defensive mechanisms. This paper aims to offer a comprehensive review of the latest research on cyber security requirements employing by machine learning techniques to tackle security issues. This demonstrates how AI and ML function in real-time cyber security, emphasizing their ability to quickly predict and prevent cyber-attacks. The findings of this study highlight the benefits and difficulties of using AI and ML in cyber security. Important areas needing careful attention include ethical issues, weaknesses due to hostile attacks and the requirement for encryption that is resistant to quantum. The paper imagines a future that combining human knowledge with AI & ML creates strong and adaptable cyber security systems.*

Keywords: *Artificial intelligent; Machine learning; real-time cyber security; Deep learning; Cyber-attacks*

Date of Submission: 14-07-2024 Date of acceptance: 31-07-2024

I. Introduction

In today's digital age, where nearly every aspect of our lives is connected to technology, the widespread presence of cyberspace has enabled unprecedented connectivity and efficiency[1]. Yet, this interconnectivity has led to a concerning increase in cyber threats, spanning from common malware to advanced, targeted attacks. As businesses move their operations online and people rely more on digital platforms, the significance of strong cyber security measures cannot be emphasized enough [1-3]. Cyber security is one of today's biggest challenges as cyber-attacks around the world keep increasing. The fast-changing nature of these threats means we need advanced technologies to strengthen defences and protect against malicious attacker[4]. The old ways of cyber security, which often depend on fixed rules and unchanging signatures, find it hard to match the fast-changing and advanced tactics used by cyber enemies[5] he threat landscape is always changing, as attackers use varied techniques like polymorphism, zero-day exploits, and social engineering, making traditional defences ineffective. In this scenario, Machine Learning (ML) integration emerges as a promising solution, bringing a new approach to cyber security[6, 7]. Machine learning, a part of artificial intelligence, enables systems to learn from data and make smart decisions without needing specific instructions for each task [8-10]. Its capacity to recognize patterns, anomalies, and trends in large datasets makes ML a valuable asset in the ongoing fight against cyber threats. Unlike traditional approaches that depend on set rules, ML algorithms can adjust and develop, giving them a strong capability to identify new and unfamiliar attack methods [11-13]. This introduction prepares for an in-depth review of how Artificial Intelligence (AI) and Machine Learning (ML) play a crucial role in real-time cyber security. In the digital age, there has been an unprecedented increase in the number and complexity of cyber-attacks[14]. As cyber-attacks become more frequent and complex, it is clear that traditional cyber security measures are not enough to protect against them. Hackers and cybercriminal groups continuously develop new methods to breach security systems. This situation underscores the need for advanced technologies like AI and ML, which can provide more dynamic and adaptive defences against cyber threats[15]. These technologies can

strengthen traditional defences and change how cyber security works by enabling threat detection and reaction in real-time. The internet world is constantly changing, with cyber threats evolving and adapting rapidly[16].

Today's sophisticated cyber-attacks are too fast for cyber security systems that were once static. Real-time cyber security is essential as threats can change in seconds, requiring a defence that can adapt just as quickly. The saying "time is of the essence" is especially true in cyber security. Detecting and responding to threats quickly is crucial to minimize harm, stop illegal access and safeguard confidential data. A threat's potential impact on systems, data integrity, and overall cyber security increases with its length of time undiscovered.

This study explores how AI and ML can transform real-time cyber security. By examining what these technologies can do and how they are used, the paper aims to show how they help in quickly identifying and addressing cyber threats as they happen. Additionally, the review aims to evaluate the effectiveness of current AI and ML methods and applications. In order to evaluate AI and ML's practicality in cyber security scenarios, the study examines examples, industry-specific applications, and success stories. This assessment sheds light on the advantages, disadvantages, and potential areas for development of the current generation of real-time cyber security technologies. Additionally, this paper wants to look closely at how AI, machine learning, and cyber security work together, especially in spotting threats and protecting against them. By knowing the problems with old methods, we can see how machine learning can make big changes.

In the following parts, we'll explore different AI and ML methods, how they're used in real-life cyber security, and the ethical concerns that come with using them.

II. Basics of AI and ML in cyber security

Understanding AI and ML fundamentals and how to apply them to enhance cyber threat identification and prevention is the first step towards integrating these technologies into cyber security [17].

Building computer systems with artificial intelligence entails making them capable of activities that often require human intelligence. AI in cyber security is capable of simulating human cognitive processes like learning, reasoning, problem-solving, and decision-making. Natural language processing, expert systems, and machine learning are important ideas. AI enhances cyber security by significantly improving traditional security methods[15].

AI can analyse large amounts of data, find patterns, and make decisions quickly, which helps deal with the fast-changing characteristics of cyber threats. AI-driven solutions increase the adaptability of cyber security strategies, allowing for proactive defences against new and evolving attack methods. ML, a branch of AI, is concerned with developing algorithms that let computers to recognize patterns in data and come to conclusions or predictions without explicit programming. Machine learning algorithms in cyber security are able to distinguish between typical activity and abnormalities, categorize dangers, and adapt to new attack patterns. ML is used in various ways in cyber security, such as:

- ✓ Detecting potential threats by identifying deviations from normal patterns.
- ✓ Examining system and user behaviour to identify odd activity.
- ✓ Identifying patterns and signatures of known cyber threats.
- ✓ Making predictions about possible weaknesses and dangers based on historical data.
- ✓ Enabling real-time automated responses to threats that are detected.

For machine learning algorithms to be used effectively in real-time cyber security operations, it is imperative that their strengths and limits are understood.

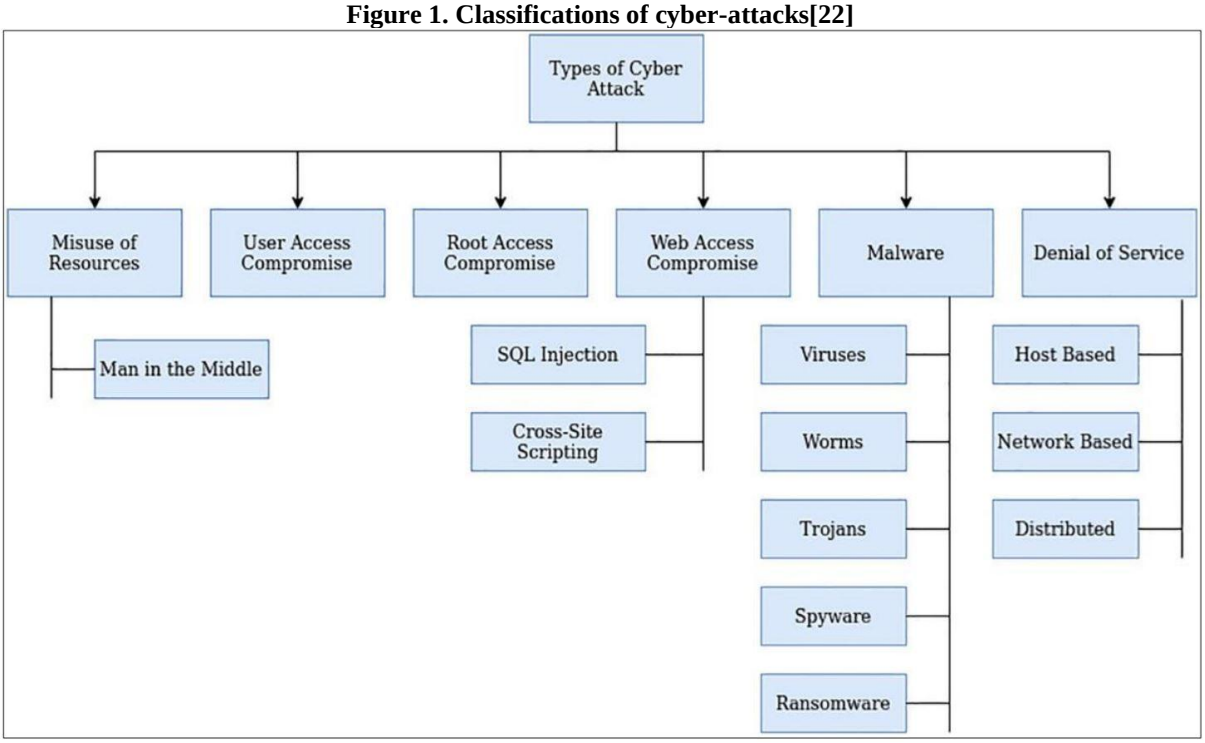
To capitalize on their distinct advantages, hybrid models incorporate both supervised and unsupervised machine learning methodologies.[18]. While unsupervised learning looks for patterns without predetermined labels, supervised learning trains on labelled datasets[19]. By combining the precision of supervised learning with the adaptability of unsupervised learning, hybrid approaches aim to increase accuracy. Ensemble models combine predictions from several machine learning models to improve strength and accuracy. Methods like bagging (Bootstrap Aggregating) and boosting combine results from different models, lessening weaknesses in individual models. Ensemble learning is especially useful in real-time cyber security as it makes threat predictions more

dependable. Knowing the basics of AI and ML sets the stage for investigating how they're used in real-time cyber security.

III. The Changing Face of Cyber Threats and How to Defend Against Them

Cyber-attacks are bad actions done on purpose to mess up computer systems, networks, and data by breaking their security, messing with their stuff, or stopping them from working. To stay safe, organizations and people use different ways to protect their digital things. Cyber threats keep changing all the time. As tech gets better and we use digital stuff more, new threats keep popping up. Some common cyber-attacks (shown in Figure 1) and ways to protect against them include malware, phishing and tricking people, advanced threats that keep going, attacks on where stuff comes from, stopping service attacks, someone getting in the middle, sneaky ways to get into databases, and tricks to mess up websites. Plus, there are new threats from people inside the organization [20, 21].

Figure 1. Classifications of cyber-attacks[22]

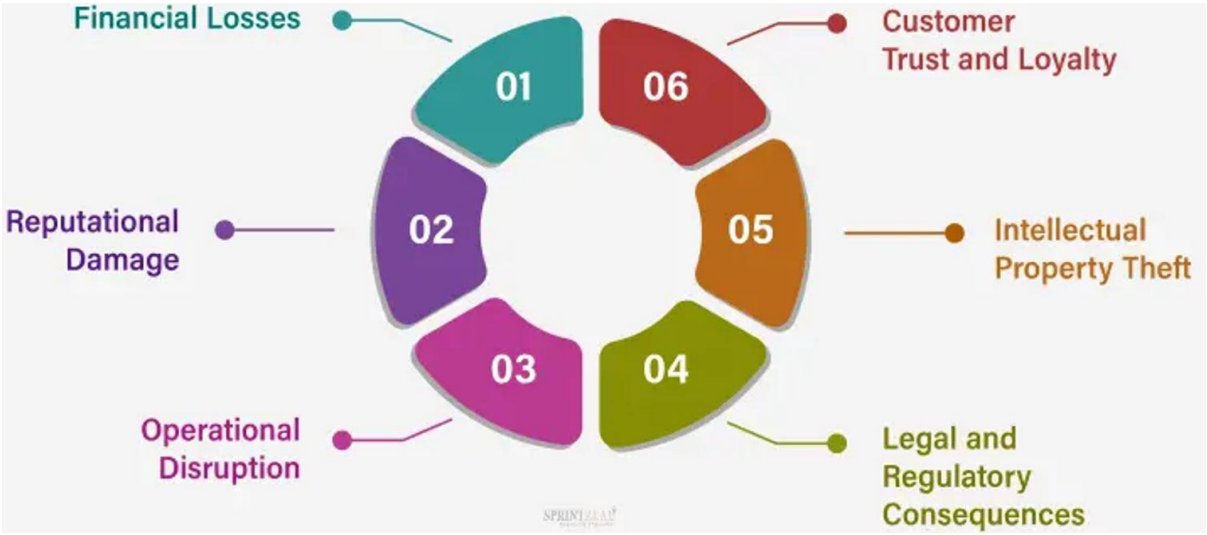


For example, bad programs like viruses, worms, and Trojan horses have been around for a long time. They can mess up computers, steal stuff, or stop them from working right. Phishing tricks people into giving away important info, like passwords or credit card numbers, by pretending to be someone you trust. Social engineering uses how people think to get them to tell secrets or do things they shouldn't[23].

Advanced persistent threats (APTs) are very sneaky and smart attacks usually done by rich and really skilled cyber bad guys, like countries. APTs try to stay in a system for a long time to spy, steal data, or mess things up. Ransom ware is a bad program that locks up someone's data and asks for money to unlock it. These attacks are getting more common and cause big problems for regular people, businesses, and even important systems[24, 25]. With more and more IoT gadgets around, there are more chances for security problems. If IoT gadgets aren't set up right or aren't protected well, they can be taken over and used to get into networks or start attacks. Instead of attacking a certain group directly, supply chain attacks mess with trusted companies that make software or hardware, so they can get into their customers' systems without permission. This can cause big problems all over the place[26]. Zero-day exploits go after weaknesses in software that the makers don't even know about yet, so there's no fix for them. Bad guys or even governments use these weak spots to get into systems without permission or put bad programs in. Insider threats are when people who are supposed to be there do bad stuff on purpose or by accident. They might give away secret stuff, mess up systems, or accidentally make things unsafe[27, 28]. As more businesses use services in the cloud, there are bigger chances for security problems like data leaks, setting things up wrong, and people getting into cloud systems without permission. Both good guys

and bad guys are using AI and machine learning to deal with security. There are attacks that mess up AI, automatic tricks to trick people into giving away info, and using AI to find weak spots and attack automatically [13, 29, 30].

Figure 2: six major impacts of cybercrime on business



To fight against these changing threats, people who work in cyber security, companies, and governments need to always change their defenses, use strong security methods, and keep learning about the newest attack tricks and trends.

Figure 3: Smart Ways to Stop Cyber Attacks

IV. Ways and models for predicting threats in real-time

Supervised Machine Learning Models: SVM is a supervised learning technique that divides data into groups by determining which hyper plane best divides each class into its component parts.[31]. SVM is good at sorting out harmful and harmless activities using labeled data. It can manage lots of data dimensions, which helps it find complicated patterns related to cyber threats. Random Forest is a method that builds many decision trees in training and picks the most common class for classification. It's great for dealing with big datasets with different characteristics. In cyber security, it's used to detect intrusions, classify malware, and spot unusual behavior[32]. Neural Networks, like the human brain, have nodes connected in layers. Deep Neural Networks adds more layers for spotting complex patterns. DNNs are good at finding detailed patterns in cyber security data, which helps detect tricky threats. They're often used for things like finding malware and incursions into networks.

Unsupervised Machine Learning Models: Finding patterns in the data is made easier by clustering algorithms, which group together comparable data points based on shared characteristics[33]. Clustering helps find oddities and put together similar cyber threats. Unsupervised clustering aids in identifying novel attack patterns in the absence of labels. Anomaly detection models identify patterns in datasets that deviate from expected behavior and may indicate potential security vulnerabilities. This detection is important for predicting threats in real-time because it helps systems spot unusual activities or patterns that could mean a cyber-attack[34]. Methods such as Isolation Forests and One-Class SVM are often used.

The goal of hybrid models is to maximize the benefits of both supervised and unsupervised learning techniques. While unsupervised learning aids in threat adaptation, supervised learning trains using labeled data. Using supervised learning for recognized hazards and unsupervised learning for identifying new ones, hybrid models provide a well-balanced combination[35]. Ensemble models bring together predictions from many models to make them more accurate and reliable. Models like bagging and boosting are key in making predictions better. By bringing together results from different models, ensemble methods fix problems in individual models and make the overall system better at predicting threats in real-time. Knowing how these methods work is important for building effective systems to predict threats quickly.

V. Real-life examples: successful uses in predicting threats as they happen

Banks and financial companies are always dealing with cybercriminals trying to get into their systems, steal data, or cheat money. They use AI and ML to spot weird things in financial transactions, which could mean someone is trying to commit fraud[36, 37].

Advanced models can spot differences in how users act, find strange transaction amounts or how often they happen, and send alerts right away for quick action. In healthcare, where there's important patient information, cyber attackers try to steal data or mess up medical services. ML algorithms are used to watch network activities in real-time, looking for anything odd that could mean a problem[34, 38]. Moreover, AI-powered predictive analytics help predict and stop planned attacks, making healthcare organizations safer from cyber threats. Vital systems like energy and transportation are at risk of cyber-attacks that can cause big problems. AI-based intrusion detection systems watch network traffic all the time, finding weird patterns and possible threats right away[39, 40]. ML models, taught with past data, help the system find new attack methods and deal with new cyber threats quickly.

A big online store is hit with a Distributed Denial of Service (DDoS) attack, which could mess up its work. Anomaly detection systems using ML watch network traffic and see a big jump in requests as something strange. The system changes its limits fast and stops the attack by sending traffic away, keeping things running for real users. A big company uses ML-based protection for its workers all over the place[41, 42]. ML algorithms keep watching how users and devices act, looking for signs something's wrong. Right away, the system separates out devices that are messed up, stopping the problem from spreading and making sure the cyber-attack doesn't mess up the whole organization's security.

6 Overview of Artificial Intelligence, Machine learning and Cyber Security Challenges and limitations

Although using (AI) and Machine Learning (ML) in cyber security has big advantages, it's important to recognize and deal with the problems and limits of these technologies. Knowing about these challenges helps make strong cyber security plans that use AI and ML well.

When a model learns the training data too much, it is said to be over fitting, picking up on noise and unimportant patterns that don't work for new, and unseen data. Over fit models might make wrong predictions, causing false alarms and extra alerts. To fix over fitting, you need strong ways to check and test the model[43, 44]. False Positives in Spotting Threats: False positives happen when a harmless thing is thought to be dangerous, which is a big problem in predicting threats as they happen. Too many false positives can tire out security teams with lots of wrong messages, making them miss real threats. To cut down on false positives, models need careful adjustments to keep up with changing threats.

Adversarial Attacks on ML Models: These attacks happen when data is changed on purpose to trick ML models into making wrong predictions[45, 46].

Attacks by adversaries can mess up how reliable ML models are, letting attackers sneak past without being noticed. It's really important to make strong models that can defend against these attacks to keep real-time threat prediction systems working well.

As there's more data and ML models get more complicated, it's hard to keep up with scalability. This can slow down how quickly big datasets are processed in real-time, which might delay predicting threats. Making algorithms better and using distributed computing resources are key to dealing with scalability problems.

Several machine learning models, especially deep neural networks, are frequently regarded as "black boxes" because of their intricate topologies[47, 48]. The problem of not being able to explain how models decide things can make it hard to trust them, especially in important situations where people need to step in. Making sure models can be explained and understood is really important for keeping things clear in real-time cybersecurity work. Dealing with these problems needs a mix of things like making algorithms stronger, making models easier to understand, and always improving based on how things go in the real world.

Model Bias and Fairness: If the data used to train a model is biased, the model might end up being biased too, which can make its predictions unfair or inaccurate. Biased models might treat different groups of people unfairly with security measures. Making sure ML models are fair means being careful about where the training data comes from and always keeping an eye out for bias[49]. Quick Changes in Cyber Threats: Cyber threats change a lot and are always getting more complicated, which makes it hard for models that stay the same to keep up in real-time. Old ML models might have trouble keeping track of new threats, showing why it's important to always train models and use techniques that can adapt quickly. Figuring out and dealing with these problems is really important for groups that want to use AI and ML as much as possible in real-time cybersecurity.

The landscape of cyber security challenges is defined by the constantly changing and evolving digital world[50]. As technology progresses, cyber threats become more advanced and complex. Factors contributing to cyber security challenges include digital transformation, which involves using adaptive cloud services, IoT devices, and interconnected systems. This expanding attack surface increases vulnerabilities, making strong security measures essential to protect digital assets and sensitive data[51, 52].

Cyber security challenges involve the threats and risks in digital security. As technology use grows and more devices become interconnected, individuals, organizations, and governments encounter many cyber security issues. These challenges come from various sources like malicious actors, human mistakes, technological weaknesses, and the constantly changing nature of cyber threats[53-56].

There has been a notable increase in cybercriminal activities worldwide[57]. Cybercriminals use different methods like phishing, ransom ware attacks, data breaches, identity theft, and financial fraud to exploit weaknesses in computer systems and networks. The financial impact of cybercrime is significant, and it keeps growing as criminals discover new ways to misuse technology[58-60].

Governments and their agencies are frequently targeted by cyber-attacks[61]. Nations engage in cyber espionage, stealing intellectual property, and sabotage to gain strategic advantages, disrupt critical infrastructure, or access sensitive information. These attacks often use advanced techniques and pose significant national security concerns. The spread of IoT devices, like smart home appliances, wearables, and industrial control systems, has introduced new security challenges. Many IoT devices have built-in vulnerabilities, and weak security can result in privacy breaches, unauthorized access, and disruptions to critical services[62, 63]. Cloud computing has changed how organizations store, process, and access data. However, it has also brought new security issues. Breaches in cloud environments can result in unauthorized access to sensitive data, service disruptions, and potential compliance violations. Organizations need strong security measures to protect their cloud infrastructure and data[64, 65]. Insider threats are security risks caused by people within an organization. These threats can come from unhappy employees, careless actions, or employees being targeted by outsiders. Insiders might intentionally or accidentally compromise systems, leak sensitive information, or engage in fraud[27]. Social engineering involves tricking people into giving out confidential information or doing things that compromise security[23]. Common techniques like phishing, pretexting, baiting, and tailgating are used to trick unsuspecting users and gain unauthorized access to systems or sensitive information[66].

Organizations must follow various data protection and privacy regulations and standards, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA)[67]. Ensuring compliance with these regulations while maintaining strong security measures is challenging, especially for multinational organizations. The quick adoption of new technologies like artificial intelligence (AI), machine learning (ML), and block chain brings both opportunities and challenges to cyber security. While these technologies can improve security, they can also be misused by cybercriminals. It's crucial to develop effective security measures for these evolving technologies [54, 66, 68].

7 Next Paths and Emerging Trends

real-time cyber security, driven by (AI) and (ML), is always changing[69]. DNNs help pull out complex details from big datasets, making it easier to spot small signs of cyber threats[32]. Progress in deep learning structures like DNNs is set to transform the prediction of immediate threats[70]. Ongoing studies to make DNNs better for cyber security will be key in making predictions more accurate. Transfer learning, a method wherein less data is used to modify already learned models for new tasks, is becoming more important in real-time cyber security. This approach helps use previous knowledge from similar areas, making it faster to adapt to new cyber threats[71]. This method makes models stronger in predicting threats in real-time situations.

It's becoming increasingly typical to combine external threat intelligence streams with AI and ML[72]. By adding up-to-date threat information, models can better grasp ongoing cyber threats. This connection allows prediction systems to adjust to the latest tactics used by enemies. Sharing anonym zed threat data amongst many businesses and industries is known as collaborative threat detection. The knowledge of evolving threats is expanded by this exchange of threat intelligence. Real-time cyber security systems can use this shared knowledge to predict and thwart attacks more effectively.

Ethical concerns are playing a bigger role in how AI and ML are used in cybersecurity[73]. Making sure that real-time threat prediction systems respect privacy, are transparent, and can be held accountable is vital. Guidelines and rules about ethics will be really important in making sure these technologies are used responsibly. When it comes to quantum computing, there's a need to pay attention to new ways of keeping information secure after quantum computers become more common[74]. Since quantum computers can crack standard encryption, it's vital to create and utilize encryption that can withstand such attacks. This will safeguard real-time threat prediction systems[75].

Continuous Adaptation and Automation: Real-time cyber security models are evolving to continuously adapt through dynamic learning[76]. By adding feedback from the actual world to the models on a regular basis, these systems are able to better adapt to changing cyber threats. It's critical to automate model changes and retraining. Autonomous response systems that use Using AI and ML to quickly respond to threats are becoming more common, reducing the need for human intervention and speeding up reduction of threats.

Interdisciplinary Research and Education: The level of collaboration among domain specialists, data scientists, and cyber security professionals is rising. By combining technological and domain-specific insights, this cross-disciplinary approach enhances the creation of comprehensive real-time threat prediction systems. The need of educating and upgrading the skills of professionals in machine learning and cyber security is also increasing. Deploying real-time threat prediction systems efficiently requires a workforce with these kinds of skills.

Explainable AI for Security Assurance: Explainable AI models are becoming more and more necessary for cyber security[77]. To foster confidence in real-time threat prediction systems, models must be comprehensible and transparent. Comprehending the decision-making process of these models is essential for fostering productive cooperation between AI and human security experts. In order to properly utilize AI and ML in anticipating and averting cyberattacks promptly, enterprises must stay abreast of emerging trends in cyber security and actively participate in research, teaching, and other activities. The future of real-time threat prediction in cyber security will be shaped by technological advancements, ethical considerations, and interdisciplinary collaboration.

8 Suggestions for Successful Implementation

An extensive set of guidelines is required in order to apply AI and ML in real-time cyber security. These cover organizational, technical, and ethical issues, guaranteeing a comprehensive strategy for applying AI and ML to quickly anticipate and stop cyber-attacks. One of the most important technical advice is to regularly monitor and assess machine learning models in order to identify biases, performance problems, and new dangers[78]. Employ automated monitoring tools to conduct routine audits, continuously assess model performance, and update models in response to evolving threat environments.

Models for real-time cyber security must be able to quickly adjust to new threats[4]. Create systems capable of dynamically updating AI and ML models to effectively combat fast-changing cyber threats. This entails establishing seamless processes for model retraining and deployment. To strengthen threat prediction models, address weaknesses by employing ensemble learning methods that amalgamate outputs from various models for increased precision and defense against harmful assaults. Making decisions in a transparent manner is essential to building understanding and confidence in real-time cyber security procedures[79]. Integrate explainable AI

methods to elucidate model decisions, encouraging cooperation for effective reaction planning between human analysts and AI systems.

To enhance cyber security, it's crucial to foster collaboration among domain experts, data scientists, and cyber security specialists[80]. Encouraging collaboration between cyber security and data science teams is vital for effective real-time threat prediction. It's important to invest in continuous training programs to keep cyber security professionals updated on AI and ML advancements. Assembling knowledgeable cross-functional teams in both fields can further enhance threat prediction capabilities. Ethical guidelines should be established to ensure responsible deployment of AI and ML technologies. Leveraging external threat intelligence by incorporating it into models for ML and AI enhances context-specific knowledge and permits more precise forecasts and anticipatory reactions.

Artificial inelegant (AI) Machine Learning (ML) includes a range of techniques and algorithms that allow systems to learn patterns, make predictions, and improve without explicit programming. Key AI &ML techniques include supervised, unsupervised, and semi-supervised learning, reinforcement learning, deep learning, neural networks, decision trees, random forests, support vector machines (SVM), and K-Nearest Neighbors (KNN). These methods are applied based on use cases like classification, clustering, and regression.

AI &ML are a powerful tool for cybersecurity threat detection. It helps develop adaptive systems that can process large data sets, recognize patterns, and identify anomalies indicating potential threats. AI &ML algorithms can analyze known malware characteristics to detect new variants. They can learn what normal behavior looks like in a system to spot deviations that may indicate attacks. AI &ML can also analyze network traffic for suspicious activities, user behavior for anomalies, and prioritize vulnerabilities based on severity.

However, AI &ML should be part of a broader security strategy, including regular updates, secure configurations, and user training. Continuous monitoring and updating of AI &ML models are necessary to adapt to evolving threats and minimize false positives or negatives[81].

9 Recommendation

Ensuring transparency in how data is utilized fosters trust among users and aligns with privacy regulations[82]. Ensuring transparency in data usage policies is vital; including clear communication with users about the kinds of data gathered, why it is collected, and security precautions. Getting the user's express consent before processing their data is crucial. Dealing with prejudices in ML models is critical for fair threat predictions, with strategies like diverse training datasets, regular fairness audits, and ongoing bias monitoring. Educating users about AI's capabilities and limitations promotes responsible usage, warranting the development of user education programs. Good communication on AI's role in danger prediction encourages human and automated system analysts to work together. Encouraging practices for responsible development among developers is necessary, emphasizing ethical implications and mechanisms for disclosing vulnerabilities. Achieving effective AI and ML implementation in cyber security requires cooperation between institutions, decision-makers, and business partners; combining organizational preparedness, technical prowess, and moral considerations to create a strong defense against changing threats.

Improving the accuracy of cyber threat identification through machine learning is an ongoing focus in research and development. Machine learning methods can bolster cyber security systems by automating the detection, classification, and response to threats. Effective machine learning models depend on diverse and training data with clear labels to identify trends and generate accurate forecasts. Having an extensive and current dataset covering various cyber threats, both established and emerging, is crucial. Identifying relevant features that aptly represent these threats is vital, drawing on cyber security expertise to select and engineer meaningful attributes. Ensemble learning, which combines multiple machine learning models, can enhance accuracy and generalization by amalgamating individual model outputs. Techniques like bagging, boosting, and stacking are employed to create robust and diverse ensembles. Anomaly detection methods, like clustering, auto encoders, and one-class SVMs, are frequently used to spot novel threats by learning from normal behavior and flagging deviations.

Deep learning models like (CNNs) and (RNNs) have proven effective in cyber security, discerning intricate patterns and relationships in data for precise threat identification. As cyber threats evolve continuously, mechanisms for continuous learning enable models to update their knowledge with real-time threat information, enhancing accuracy in detecting emerging threats.

Adversarial attacks aim to circumvent machine learning models, prompting the development of resilient models through adversarial machine learning techniques like adversarial training and defensive distillation. While machine learning models automate and augment threat identification, human expertise remains indispensable. Integrating human input and domain knowledge can validate and interpret model predictions, refining accuracy and minimizing false positives/negatives.

Regular evaluation of machine learning model performance is crucial for refinement, with feedback from analysts and cybersecurity experts informing model enhancements over time. It's essential to remember that while machine learning greatly enhances cyber threat identification, it should be part of a comprehensive cybersecurity framework integrating other techniques like network monitoring, intrusion detection systems, secure coding practices, and user awareness training.

10 Conclusion

Investigating AI and ML for cyber security in real-time uncovers both opportunities and challenges. This study extensively examines their potential for predicting and preventing cyber-attacks promptly. It underscores the need for innovative approaches to bolster cyber security, since dynamic reaction mechanisms and adaptive threat detection are promised by AI and ML. However, integrating these technologies faces hurdles like ethical concerns; explain ability issues, and the persistent threat of adversarial attacks. Overcoming these challenges demands a balanced and intentional approach. In the future, study endeavors are focused on enhancing explain ability, fortifying security against hostile assaults, and bridging the divide between artificial intelligence and human proficiency. Collaboration among researchers, practitioners, and policymakers is vital for shaping the future of AI-driven cyber security. By combining human knowledge with AI and ML capabilities, resilient and reliable cyber security ecosystems can be established to safeguard our digital realm. Continuous pursuit of learning and innovation remains essential in this endeavor.

The adoption of AI &ML in proactive defense strategies signifies a transformative shift in cyber security. AI &ML's utilization of advanced analytics and pattern recognition enhances defense capabilities by enabling smarter, more adaptive, and efficient responses. Its capacity to identify subtle anomalies, automate actions, and continuously learn from evolving threats positions AI &ML as a cornerstone of modern cyber security approaches. Leveraging ML and AI algorithms allows for the analysis of vast datasets detecting patterns, anomalies, and previously unidentified threats. Through training on historical data, AI &ML models can recognize known threat patterns, progressively improving accuracy over time.

In summary, while challenges persist, integrating ML & AI into proactive defense mechanisms is crucial for organizations seeking to outmaneuver cyber adversaries. As the field evolves, addressing concerns and leveraging AI& ML's strengths will be essential to fully realizing its potential in bolstering cyber security defenses.

References

[1]. Kearney, M.R., Navigating the Eisenhower Interstate System: Paving the way for cyberspace. Explorations in Media Ecology, 2023. **22**(1): p. 33-48.

[2]. Nassar, A. and M. Kamal, Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies. Journal of Artificial Intelligence and Machine Learning in Management, 2021. **5**(1): p. 51-63.

[3]. Abdel-Rahman, M., Advanced cybersecurity measures in IT service operations and their crucial role in safeguarding enterprise data in a connected world. Eigenpub Review of Science and Technology, 2023. **7**(1): p. 138-158.

[4]. George, A.S., Securing the future of finance: how AI, Blockchain, and machine learning safeguard emerging Neobank technology against evolving cyber threats. Partners Universal Innovative Research Publication, 2023. **1**(1): p. 54-66.

[5]. Möller, D.P., Cybersecurity in digital transformation, in Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices. 2023, Springer. p. 1-70.

[6]. Aiyanyo, I.D., H. Samuel, and H. Lim, A systematic review of defensive and offensive cybersecurity with machine learning. Applied Sciences, 2020. **10**(17): p. 5811.

[7]. Bresniker, K., et al., Grand challenge: Applying artificial intelligence and machine learning to cybersecurity. Computer, 2019. **52**(12): p. 45-52.

[8]. Raschka, S., J. Patterson, and C. Nolet, Machine learning in python: Main developments and technology trends in data science, machine learning, and artificial intelligence. Information, 2020. **11**(4): p. 193.

[9]. Chinesta, F. and E. Cueto, Empowering engineering with data, machine learning and artificial intelligence: a short introductive review. Advanced Modeling and Simulation in Engineering Sciences, 2022. **9**(1): p. 21.

[10]. Nassehi, A., et al., Review of machine learning technologies and artificial intelligence in modern manufacturing systems, in Design and operation of production networks for mass personalization in the era of cloud technology. 2022, Elsevier. p. 317-348.

[11]. Anamu, U., et al., Fundamental design strategies for advancing the development of high entropy alloys for thermo-mechanical application: A critical review. Journal of Materials Research and Technology, 2023.

[12]. Wang, Y., et al., Adversarial attacks and defenses in machine learning-empowered communication systems and networks: A contemporary survey. IEEE Communications Surveys & Tutorials, 2023.

[13]. Bout, E., V. Loscri, and A. Gallais, How machine learning changes the nature of cyberattacks on IoT networks: A survey. IEEE Communications Surveys & Tutorials, 2021. **24**(1): p. 248-279.
[14]. Lallie, H.S., et al., Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & security, 2021. **105**: p. 102248.
[15]. Kumar, S., et al., Artificial intelligence: revolutionizing cyber security in the digital era. Journal of Computers, Mechanical and Management, 2023. **2**(3): p. 31-42.
[16]. Sadik, S., et al., Toward a sustainable cybersecurity ecosystem. Computers, 2020. **9**(3): p. 74.
[17]. Li, J.-h., Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 2018. **19**(12): p. 1462-1474.
[18]. Liu, H. and B. Lang, Machine learning and deep learning methods for intrusion detection systems: A survey. applied sciences, 2019. **9**(20): p. 4396.
[19]. Reddy, Y., P. Viswanath, and B.E. Reddy, Semi-supervised learning: A brief review. Int. J. Eng. Technol, 2018. **7**(1.8): p. 81.
[20]. Dobák, I., Thoughts on the evolution of national security in cyberspace. Security and Defence Quarterly, 2021. **33**(1): p. 75-85.
[21]. Kopczewski, M., et al., Security threats in cyberspace. Scientific Journal of the Military University of Land Forces, 2022. **54**.
[22]. Al-Enezi, K.A., et al. A survey of intrusion detection system using case study Kuwait Governments entities. in 2014 3rd International Conference on Advanced Computer Science Applications and Technologies. 2014. IEEE.
[23]. Syafitri, W., et al., Social engineering attacks prevention: A systematic literature review. IEEE access, 2022. **10**: p. 39325-39343.
[24]. Sharma, A., et al., Advanced Persistent Threats (APT): evolution, anatomy, attribution and countermeasures. Journal of Ambient Intelligence and Humanized Computing, 2023. **14**(7): p. 9355-9381.
[25]. Teichmann, F., S.R. Boticiu, and B.S. Sergi, The evolution of ransomware attacks in light of recent cyber threats. How can geopolitical conflicts influence the cyber climate? International Cybersecurity Law Review, 2023. **4**(3): p. 259-280.
[26]. Li, Z., et al., Security threat model under internet of things using deep learning and edge analysis of cyberspace governance. International Journal of System Assurance Engineering and Management, 2022. **13**(Suppl 3): p. 1164-1176.
[27]. Yuan, S. and X. Wu, Deep learning for insider threat detection: Review, challenges and opportunities. Computers & Security, 2021. **104**: p. 102221.
[28]. Саприкін, О.С., Models and methods for diagnosing Zero-Day threats in cyberspace. Вісник сучасних інформаційних технологій, 2021. **4**(2): p. 155-167.
[29]. Panem, C., S.R. Gundu, and J. Vijaylaxmi, The Role of Machine Learning and Artificial Intelligence in Detecting the Malicious Use of Cyber Space. Robotic Process Automation, 2023: p. 19-32.
[30]. Malaviya, D., Application of machine learning and artificial intelligence for securing cyber space and the role of government organization. Anusandhaan-Vigyaan Shodh Patrika, 2022. **10**(01): p. 33-37.
[31]. Amarappa, S. and S. Sathyanarayana, Data classification using Support vector Machine (SVM), a simplified approach. Int. J. Electron. Comput. Sci. Eng, 2014. **3**: p. 435-445.
[32]. Bouchama, F. and M. Kamal, Enhancing Cyber Threat Detection through Machine Learning-Based Behavioral Modeling of Network Traffic Patterns. International Journal of Business Intelligence and Big Data Analytics, 2021. **4**(9): p. 1-9.
[33]. Chaudhry, M., et al., A systematic literature review on identifying patterns using unsupervised clustering algorithms: A data mining perspective. Symmetry, 2023. **15**(9): p. 1679.
[34]. Habeeb, R.A.A., et al., Real-time big data processing for anomaly detection: A survey. International Journal of Information Management, 2019. **45**: p. 289-307.
[35]. Zhou, L., et al., Machine learning on big data: Opportunities and challenges. Neurocomputing, 2017. **237**: p. 350-361.
[36]. Ahmed, M., A.N. Mahmood, and M.R. Islam, A survey of anomaly detection techniques in financial domain. Future Generation Computer Systems, 2016. **55**: p. 278-288.
[37]. Adaga, E.M., et al., Philosophy in business analytics: a review of sustainable and ethical approaches. International Journal of Management & Entrepreneurship Research, 2024. **6**(1): p. 69-86.
[38]. Abrahams, T.O., et al., Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security. 2023.
[39]. Markevych, M. and M. Dawson. A review of enhancing intrusion detection systems for cybersecurity using artificial intelligence (ai). in International conference Knowledge-based Organization. 2023.
[40]. Vincent, A.A., et al., Entrepreneurship, agricultural value-chain and exports in Nigeria. United International Journal for Research and Technology, 2021. **2**(08): p. 1-8.
[41]. Kak, S., Zero Trust Evolution & Transforming Enterprise Security. 2022, California State University San Marcos.
[42]. Abrahams, T.O., et al., Mastering compliance: a comprehensive review of regulatory frameworks in accounting and cybersecurity. Computer Science & IT Research Journal, 2024. **5**(1): p. 120-140.
[43]. Montesinos López, O.A., A. Montesinos López, and J. Crossa, Overfitting, model tuning, and evaluation of prediction performance, in Multivariate statistical machine learning methods for genomic prediction. 2022, Springer. p. 109-139.
[44]. Hassan, A.O., et al., Cybersecurity in banking: a global perspective with a focus on Nigerian practices. Computer Science & IT Research Journal, 2024. **5**(1): p. 41-59.
[45]. Radanliev, P. and O. Santos, Adversarial Attacks Can Deceive AI Systems, Leading to Misclassification or Incorrect Decisions. 2023.
[46]. Balogun, O.D., et al., The Role of pharmacists in personalised medicine: a review of integrating pharmacogenomics into clinical practice. International Medical Science Research Journal, 2024. **4**(1): p. 19-36.
[47]. Buhrmester, V., D. Münch, and M. Arens, Analysis of explainers of black box deep neural networks for computer vision: A survey. Machine Learning and Knowledge Extraction, 2021. **3**(4): p. 966-989.
[48]. Akindote, O.J., et al., Comparative review of big data analytics and GIS in healthcare decision-making. World Journal of Advanced Research and Reviews, 2023. **20**(3): p. 1293-1302.
[49]. Mehrabi, N., et al., A survey on bias and fairness in machine learning. ACM computing surveys (CSUR), 2021. **54**(6): p. 1-35.
[50]. Nguyen, M.T. and M.Q. Tran, Balancing security and privacy in the digital age: an in-depth analysis of legal and regulatory frameworks impacting cybersecurity practices. International Journal of Intelligent Automation and Computing, 2023. **6**(5): p. 1-12.
[51]. Djenna, A., S. Harous, and D.E. Saidouni, Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences, 2021. **11**(10): p. 4580.
[52]. Lakhani, A., AI Revolutionizing Cyber security unlocking the Future of Digital Protection. 2023.
[53]. Krause, T., et al., Cybersecurity in power grids: Challenges and opportunities. Sensors, 2021. **21**(18): p. 6225.
[54]. Bechara, F.R. and S.B. Schuch, Cybersecurity and global regulatory challenges. Journal of Financial Crime, 2021. **28**(2): p. 359-374.
[55]. Akpan, F., et al., Cybersecurity challenges in the maritime sector. Network, 2022. **2**(1): p. 123-138.

[56]. Tufail, S., et al., A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid. Energies, 2021. **14**(18): p. 5894.
[57]. Gangwar, S. and V. Narang, A survey on emerging cyber crimes and their impact worldwide, in Research Anthology on Combating Cyber-Aggression and Online Negativity. 2022, IGI Global. p. 1583-1595.
[58]. Sarkar, G., et al. Tactics, techniques and procedures of cybercrime: A methodology and tool for cybercrime investigation process. in Proceedings of the 18th International Conference on Availability, Reliability and Security. 2023.
[59]. Bada, M. and J.R. Nurse. Profiling the cybercriminal: A systematic review of research. in 2021 international conference on cyber situational awareness, data analytics and assessment (CyberSA). 2021. IEEE.
[60]. Sarkar, G. and S.K. Shukla, Behavioral analysis of cybercrime: Paving the way for effective policing strategies. Journal of Economic Criminology, 2023: p. 100034.
[61]. Chigada, J. and R. Madzinga, Cyberattacks and threats during COVID-19: A systematic literature review. South African Journal of Information Management, 2021. **23**(1): p. 1-11.
[62]. Alsheikh, M., et al., The state of IoT security: Unequivocal appeal to cybercriminals, onerous to defenders. IEEE Consumer Electronics Magazine, 2021. **11**(3): p. 59-68.
[63]. Fortino, G., et al., Iot platforms and security: An analysis of the leading industrial/commercial solutions. Sensors, 2022. **22**(6): p. 2196.
[64]. Frank, R., G. Schumacher, and A. Tamm, The cloud transformation, in Cloud Transformation: The Public Cloud Is Changing Businesses. 2023, Springer. p. 203-245.
[65]. Berisha, B., E. Mëziu, and I. Shabani, Big data analytics in Cloud computing: an overview. Journal of Cloud Computing, 2022. **11**(1): p. 24.
[66]. Okoli, U.I., et al., Machine learning in cybersecurity: A review of threat detection and defense mechanisms. 2024.
[67]. Mulgund, P., et al., The implications of the California Consumer Privacy Act (CCPA) on healthcare organizations: Lessons learned from early compliance experiences. Health Policy and Technology, 2021. **10**(3): p. 100543.
[68]. Mishra, A., et al., Cybersecurity enterprises policies: A comparative study. Sensors, 2022. **22**(2): p. 538.
[69]. Babu, C.S., Adaptive AI for Dynamic Cybersecurity Systems: Enhancing Protection in a Rapidly Evolving Digital Landscap, in Principles and Applications of Adaptive Artificial Intelligence. 2024, IGI Global. p. 52-72.
[70]. Kim, A., M. Park, and D.H. Lee, AI-IDS: Application of deep learning to real-time Web intrusion detection. IEEE Access, 2020. **8**: p. 70245-70261.
[71]. Ali, S.M., J.C. Augusto, and D. Windridge, A survey of user-centred approaches for smart home transfer learning and new user home automation adaptation. Applied Artificial Intelligence, 2019. **33**(8): p. 747-774.
[72]. Tounsi, W. and H. Rais, A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security, 2018. **72**: p. 212-233.
[73]. Al-Mansoori, S. and M.B. Salem, The role of artificial intelligence and machine learning in shaping the future of cybersecurity: trends, applications, and ethical considerations. International Journal of Social Analytics, 2023. **8**(9): p. 1-16.
[74]. Bernstein, D.J. and T. Lange, Post-quantum cryptography. Nature, 2017. **549**(7671): p. 188-194.
[75]. Khan, W.Z., M. Raza, and M. Imran, Quantum Cryptography a Real Threat to Classical Blockchain: Requirements and Challenges. Authorea Preprints, 2023.
[76]. Hatzivasilis, G., et al., Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. Applied Sciences, 2020. **10**(16): p. 5702.
[77]. Sharma, D.K., et al., Explainable artificial intelligence for cybersecurity. Computers and Electrical Engineering, 2022. **103**: p. 108356.
[78]. Angelopoulos, A., et al., Tackling faults in the industry 4.0 era—a survey of machine-learning solutions and key aspects. Sensors, 2019. **20**(1): p. 109.
[79]. Nyre-Yu, M., et al., Explainable AI in Cybersecurity Operations: Lessons Learned from xAI Tool Deployment. 2022, Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).
[80]. Cains, M.G., et al., Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. Risk Analysis, 2022. **42**(8): p. 1643-1669.
[81]. Sarker, I.H., Machine learning: Algorithms, real-world applications and research directions. SN computer science, 2021. **2**(3): p. 160.
[82]. Richards, N. and W. Hartzog, Privacy's trust gap: a review. 2016, HeinOnline.