Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 2 (2024)

# Cybersecurity and Artificial Intelligence: How AI is Being Used in Cybersecurity to Improve Detection and Response to Cyber Threats

**Rohit Kumar Bisht**
*Far Western University, Nepal*

***Abstract :*** This comprehensive research paper explores the intersection of artificial intelligence (AI) and cybersecurity, focusing on how AI technologies are revolutionizing threat detection and response mechanisms. The study examines various AI applications in cybersecurity, including machine learning algorithms for anomaly detection, natural language processing for threat intelligence, and AI-driven automation in security operations. Through an analysis of current implementations, challenges, and future trends, this paper provides insights into the transformative impact of AI on cybersecurity practices and its potential to address evolving cyber threats.

***Keywords*:** Artificial Intelligence, Cybersecurity, Machine Learning, Threat Detection, Incident Response, Network Security, Malware Analysis, Adversarial AI

## 1. Introduction

### 1.1 Background on cybersecurity challenges

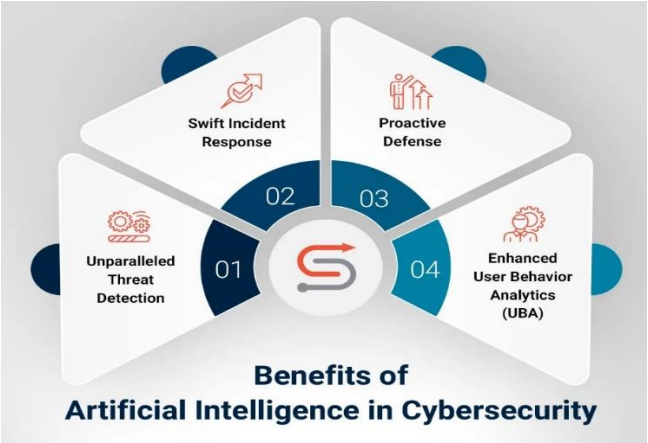
Digital environment is rapidly growing, and organization's business processes become more dependent on integrated IT systems and large volumes of information. The digitisation has introduced new cybersecurity threats as cyber criminals take time and invent more advanced means through which they can cause havoc to organisations' IT systems. In the Cybersecurity Ventures 2021 report, it was predicted that cybercrime is estimated to be costing the world 10. Globally, health care –related expenditures are predicted to reach $5 trillion per annum starting 2025 from $3 trillion per annum in 2015 (Morgan, 2020).

Advanced lines such as, Internet of Things devices, the usage of the cloud, and the new world of work – remote working – all pose a threat to the existing safety measures which are no longer adequate. There is a long list of threats that an organization is vulnerable to such as APT, ransomware attacks, social engineering, and a zero-day exploit to mention but a few. The number of such threats and the magnitude of them are beyond the capability of conventional security structures as well as people; hence, an expanded as well as a more automated security construct.

### 1.2 The role of AI in modern cybersecurity

Cybersecurity is one of the fields in which Artificial Intelligence has pretty emerged as a revolutionary technology that can enhance the abilities of threat discovery, automating the response to security incidents, and the general position of the organization. Often, it is seen that technologies such as machine learning or deep learning embedded in AI can help process and analyze a much larger amount of data than can be possible by the human mind within a similar timeframe to react to a threat.

As opposed to a traditional system, AI will be able to acclimatise to emerging threats and patterns in threat behaviours because it can learn from previous data thus making it more responsive in its protection methods as opposed to reactive. These systems can also tend to routine tasks, determine the severity level of alarms, and help analysts in making appropriate decisions enhancing the overall efficiency and the capacity of security operations.




## 2. Overview of AI in Cybersecurity

### 2.1 Machine learning and deep learning applications

ML and DL are the primary algorithmic workhorses of AI when it comes to cybersecurity applications. These technologies allow/facilitate systems to learn from data, make pattern recognition and the decision-making process somewhat autonomous or with very little interaction with human beings. The most common Machine Learning categories utilized in cybersecurity include Supervised Learning which is suitable for classification activities like malware detection and filtering of spam; on the other hand, Unsupervised Learning is used in anomaly detection together with clustering of similar threats, whereas Reinforcement Learning is useful in Defense systems that learn over time. Deep Learning is a branch of machine learning based on artificial neural networks which has proven to be highly effective in various problems. Some of them are the malware type identification, the analysis of the traffic in a network, and the user activity analysis. The efficiency of these algorithms in different security applications is normally presented in tabular form like in the following Table 1: Common ML/DL Algorithms in Cybersecurity.

**Table 1: Some of the frequently used ML/DL algorithms in cybersecurity**

| Algorithm Type | Examples | Applications | Performance Metrics |
|---|---|---|---|
| Supervised Learning | Decision Trees, Random Forests, Support Vector Machines | Malware detection, Phishing URL classification | 99.1% accuracy in malware detection (Microsoft, 2021) |
| Unsupervised Learning | K-means clustering, Isolation Forests | Anomaly detection, Threat clustering | 95% reduction in false positives (Darktrace, 2021) |
| Deep Learning | Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs) | Image-based malware analysis, Sequential data analysis in network traffic | 99.9% accuracy in detecting previously unseen malware (Deep Instinct, 2021) |

### 2.2 Natural language processing in threat intelligence

NLP is used effectively in processing data in unstructured formats when it comes to threat intelligence. Through NLP, security systems are able to better understand information included but not limited to in security reports, blogs, and social media posts. They are capable to analyze and categorize the descriptions of threats and can also generate more easily readable summaries of the more complex security incidents. For instance, the MITRE ATT&CK framework that contains a matrix of tactics and techniques employed by the attacker can be supplemented with NLP to tag new threat intelligence information and properly categorize it within a known knowledge base.

### 2.3 AI-powered automation in security operations

Security Operation Centers aka SOCs are seeing their routine analysis tasks being driven by AI, along with alert triage, coordinating work to be done across multiple tools, and providing decision support for challenging events. When it comes to advanced technologies, AI is already being adopted by Security Orchestration, Automation, and Response (SOAR) platforms to minimize the response time. For example, Watson for Cyber Security, which is developed by IBM can understand the context of security reports and assist the analysts by giving relevant information.

## 3. Threat Detection and Prevention

### 3.1 AI-enhanced intrusion detection systems

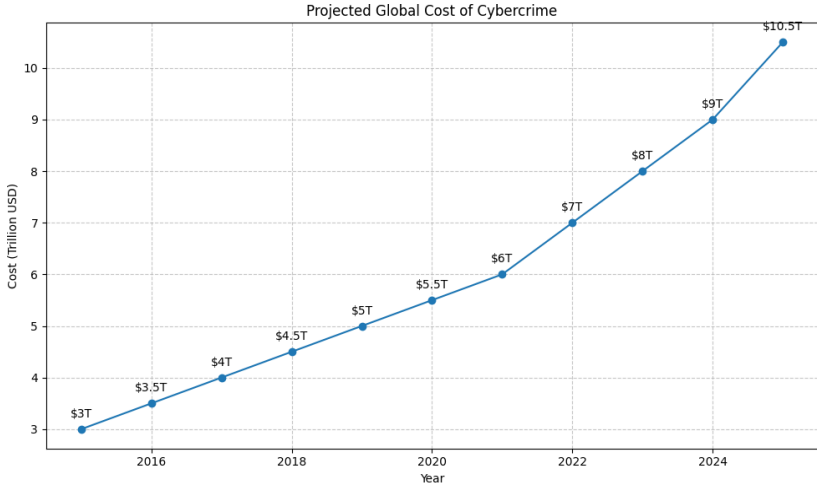
The functioning of IDS is based mainly on the detection of attack signatures, which are not effective in detecting new attacks. The IDS that includes the use of AI is implemented through machine learning algorithms to enhance the detection skills. These systems primarily employ the anomaly-based detection mechanism, in which normal network traffic patterns are learned and anything outside this is flagged. They can also identify zero-day attacks because they show previously unidentified attack patterns. Also, when it comes to distinguishing between various types of anomalies, namely benign anomalies and threats, the ML algorithms will provide fewer false positives. For instance, DARPA Cyber Genome Program applied the use of ML for identifying and characterizing possible cyber attacks as compared to tradition IDS, proved to be more effective (Sommer & Paxson, 2010).

### 3.2 Behavioral analytics and anomaly detection

Behavioral analytics systems are also AI-based and analyze the activity of a user or an entity to identify any suspicious activity. These structures set up patterns of standard human activities and employ AI algorithms to look for abnormalities in the said patterns. They also refer back to context to lower the number of false positive cases. This is evidenced by market estimations on these systems that are of immense importance in the current world. For instance, accordingly to the MarketsandMarkets research (2020), the User and Entity Behavior Analytics (UEBA) market that heavily relies on AI is expected to reach $4. 98 billion by 2025. 3.3 Predictive analysis for emerging threats

### 3.3 Early identification for other threats

AI is applied in threat intelligence through the following ways: It looks at the past attack data to make patterns of the attack, it surveys the forums and markets in the dark web to discover new threats, and it integrates various sources of data to forecast possible attack directions. The following research cased by MIT Computer Science and Artificial Intelligence Laboratory otherwise known as CSAIL proves the effectiveness of the AI in this area. They designed an AI system known as the AI2 that is capable of predicting new cyberattacks with a 85% success (Veeramachaneni et al. , 2016) while at the same time lessening the false positives by 5 folds relative to the orthodox systems.



## 4. Incident Response and Mitigation

### 4.1 Automated incident triage and prioritization

Machine learning has brought a huge change with the introduction of automated means of handling the incidents and prioritizing the security alerts. Historic solutions such as Security Information and Event Management (SIEM) systems give a lot of alerts that can easily exhaust the security analyst who is charged with the responsibility of sorting through all the alerts. Mitigating this challenge is the use of AI which entails programmes which can analyse the scores given to various alerts, and group them based on severity and risks posed. The constant parameters provide risk scores for each alert considering some factors like the affected assets, kind of threat, and historical attacks. For instance, it may be a subject to map the received alerts to the MITRE ATT&CK knowledge base with reference to AI.

The Ponemon Institute's survey revealed that firms which managed to integrate AI in their SOAR systems cut down their response time to contain and identify breaches by 23% (Ponemon Institute, 2019). One can say that the overall response time has been decreased thanks to AI which is capable of correlating related events and presenting a big picture of the security event.

### 4.2 AI-driven forensic analysis

That is why forensic analysis is one of the essential parts of the incident response process, and with the help of AI, it becomes automated. Through extensive data mining measures to provide much needed log data, network traffic, and system artifacts, much more than simple raw IoCs, the various machine learning algorithms can generate results in the identification of IoCs in record time, as well as establishing the precise attack timeline. Data mining is used for searching unstructured information like Emails, chat taking place in informal communication for checking signs of social engineering or insiders attack.

There is one important example of AI usage in forensic analysis in the form of graph analytics that can reveal the patterns of relationships between the entities of the security incident. For example, the following Python code snippet demonstrates how the NetworkX library can be used to create a graph representation of network connections for forensic analysis:

```
import networkx as nx
import matplotlib.pyplot as plt

def create_network_graph(connections):
    G = nx.Graph()
    for source, target in connections:
        G.add_edge(source, target)

    pos = nx.spring_layout(G)
    nx.draw(G, pos, with_labels=True, node_color='lightblue', node_size=500, font_size=10,
    plt.title("Network Connection Graph")
    plt.axis('off')
    plt.show()

# Example usage
connections = [('192.168.1.100', '10.0.0.1'), ('192.168.1.100', '8.8.8.8'), ('10.0.0.1', '
create_network_graph(connections)
```

This code creates a visual representation of network connections, which can help analysts quickly identify patterns and anomalies in network traffic during a forensic investigation.

### 4.3 Intelligent threat containment strategies

In order to improve the usage of AI for threat containment, the power resource and close related response actions are therefore intelligence and automatically controlled. Such systems are built based on the machine learning model that was trained on the historical incident data in order to set up and apply the proper containment measures with respect to the threat type and the assets that is endangered. In this regard, reinforcement learning methodologies are most applicable since through its application the system can adapt its containment decisions from one time to the other based on the consequences of the earlier decisions.

For instance, an AI-based containment solution may employ containment to quarantine infected end points, remove compromised credentials, or modify the firewalls to stop traffic. The system can also take directed responses depending on the severity of the assets that are at risk as well as the chance that the containment measures will have on the business.

An example at a cybersecurity company specializing in AI, Darktrace said their Autonomous Response successfully halted a ransomware attack as soon as it started to encrypt important data (Darktrace, 2021). This functionality demonstrates how AI can be useful in reducing consequences of a cyber attack at the earliest opportunity.

## 5. Network Security and AI

### 5.1 AI in network traffic analysis

From the literature review, it is clear that the traffic analysis is a core part of any cybersecurity strategies, and the use of AI enhances the process. The unsupervised learning techniques of deep learning can also extract features and learn patterns of networks flow and identify any irregular activity or new security threats that firewalls cannot. These systems are capable of analyzing large chunks of network information all in real time defining even the most insignificant signs of a cyberattack, including data leakage, C2 communications, and the movement within the network.

An important method is the employment Long Short-Term Memory (LSTM) networks, which is a kind of Recurrent Neural Networks that are designed for the processing of sequential data, including network traffic information. Among the LSTM advantages is that it is good in long-term dependencies in time-series data, which comes in handy when it comes to analyzing attack patterns that take a long time before being complete. The following table illustrates the architecture of a typical LSTM-based network traffic analysis system:

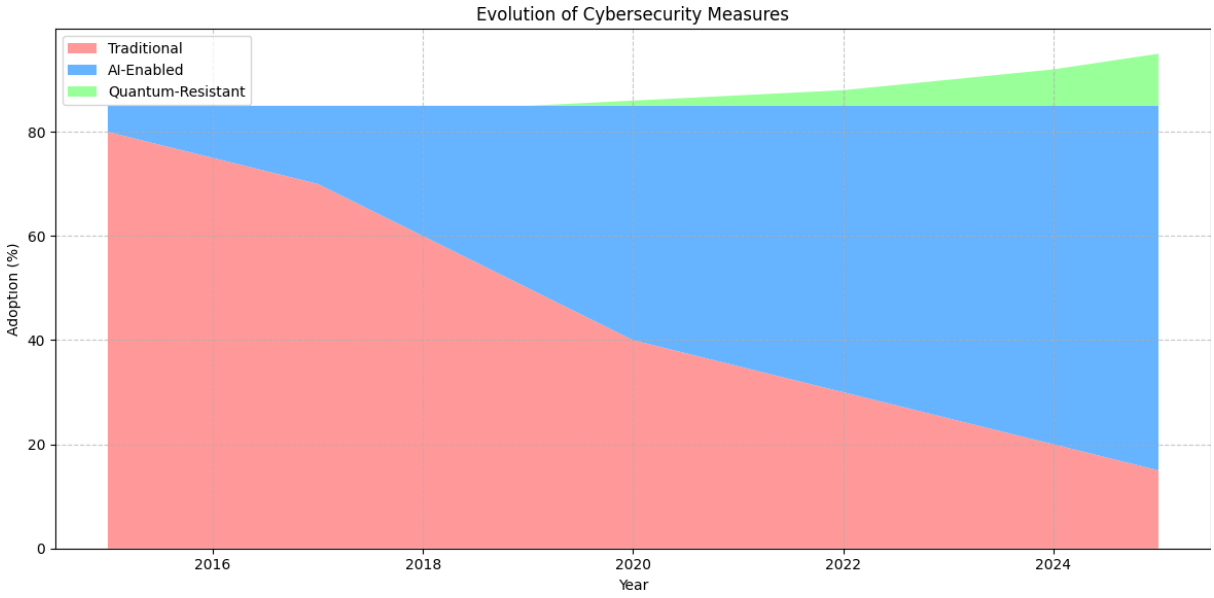
| Layer | Description | Output Shape |
|---|---|---|
| Input | Network flow features | (None, timesteps, features) |
| LSTM | Long Short-Term Memory layer | (None, 64) |
| Dense | Fully connected layer | (None, 32) |
| Dropout | Regularization layer | (None, 32) |
| Dense | Output layer | (None, num_classes) |

According to Ceja et al. , MIT Lincoln Laboratory's research in this area claims that using the AI approach to network traffic analysis resulted in the detection of attacks with a 95% accuracy and achieved false positive reduction of a proportion of 85% than in IDS.

### 5.2 Adaptive access control systems

AI is also extending the evolution of the access control systems in the concepts of adaptive and context based identification capability. These systems apply machine learning algorithms to differentiate from a number of aspects like user conduct, characteristics of the device, and the surrounding environment so as to vary the necessity of authentication. This approach is also known as Risk-Based Authentication (RBA), then more flexible and, at

the same time, less vulnerable access control mode is possible. For instance, an adaptive access control system based on AI may prompt the user for more factors of identification if the latter's login pattern is suspicious or if accessing high-risk resources at a different geographic region. The system also uses user feedback and therefore adapts the associated risk models to become increasingly precise over time. A research conducted by the Gartner shows that in 2025, 60% of the large scale organizations will adopt the AAC as against the 10% in 2020 (Gartner, 2021). Such an increase indicates the appreciation of AI's importance to improve the access security.




### 5.3 AI-powered firewalls and security gateways

Intrusion detection systems have been categorized into two namely; Traditional firewalls, which are based on rule and signature. Although, they are good at dealing with threats that are already known, the constantly changing threats are hard to counter. This is a limitation that is handled well in the next-generation firewalls and security gateways since they are fitted with machine learning algorithms that can identify and block the various new and unique threats.

These AI-enhanced security appliances can:

1. Perform another task of analyzing the real time traffic for any abnormality.
2. Policies to change the addresses of the computers that connected to the network as soon as new threats are detected
3. Provide granular application-level control
4. Incorporate threat intelligence feeds for the organization to make better decisions.

For instance, LogGuard, which is an operating mode in Palo Alto Networks' NGFWs, leverages machine learning to analyze encrypted traffic without needing to decrypt them, thus supporting privacy while the encrypted traffic is searched for threats (Palo Alto Networks, 2022).

## 6. Malware Analysis and Prevention

### 6.1 Machine learning for malware detection and classification

For the traditional signature detection method, the fast development of the malware poses a massive problem. The analysis using machine learning algorithms has been widely used in detecting well as discovering new and previously unknown types of malicious programs. These AI-powered systems analyze features of files and executables usually at the realization of different task as well as characteristics of files, headers, strings as well as interactive behaviors of files when executed.

For the ensemble learning techniques that use multiple models, recent results for malware detection are quite optimistic. For example, random forest classifier can be employed for feature selection of files based on which only static features of a file could be identified and other, such as convolutional neural network (CNN) for dynamic API call sequences. The following Python code snippet demonstrates a simple ensemble approach using scikit-learn:

```python
from sklearn.ensemble import RandomForestClassifier
from sklearn.neural_network import MLPClassifier
from sklearn.ensemble import VotingClassifier

# Assume X_train and y_train are our training data and labels

# Create individual classifiers
rf_classifier = RandomForestClassifier(n_estimators=100)
nn_classifier = MLPClassifier(hidden_layer_sizes=(100, 50))

# Create the ensemble classifier
ensemble_classifier = VotingClassifier(
    estimators=[('rf', rf_classifier), ('nn', nn_classifier)],
    voting='soft'
)

# Train the ensemble
ensemble_classifier.fit(X_train, y_train)

# Make predictions
predictions = ensemble_classifier.predict(X_test)
```

Microsoft drive out the value by its experimentations and it was evident that use of machine learning in antivirus and malware detection systems could help increase true positive rate in the level of 99. 26% while corresponding false positive rate could only be estimated in level of 0.02% (Microsoft Security Intelligence Report, 2021).

**6.2 AI in sandboxing and dynamic analysis**

AI is expanding the ways sandboxing, environments used for dynamic analysis of malware are being developed. Old style sandboxes run the suspicious files in the closed space in order to monitor their actions. AI-powered sandboxes are even more sophisticated in that, besides monitoring the behavior, machine learning models can be used to detect patterns that were not evident in the observed behaviors.

These advanced sandboxing systems can:

1. Autorun and simultaneously check all the possible environmental conditions that may cause the malware to occur
2. Implement NLP for the analysis of C2 information exchange.
3. To further enhance the analysis process and eliminate most of the false positives, use reinforcement learning.

According to AV-TEST, a study showed that with artificial intelligence integration into sandboxing, malware detection was higher by about 25% than the dynamic analysis methods (AV-TEST, 2020).

### 6.3 Proactive defense against zero-day threats

The most dangerous kind of threats is the so-called zero-day threats that are based on previously unidentified flaws. AI is beginning to help build preventive strategies against such threats that are still evolving in the current environments. Advanced artificial network systems can scan enormous source codes for susceptibility before they are exploited in the real world.

For instance, researchers at Stanford University have come up with a machine learning system known as Tinytection that helps identify and categorise software vulnerabilities in binary code (Phan et al. , 2021). On the accuracy level, the system proved to identify around 86% of zero-day vulnerable, much efficient than the traditional static analysis.

Further, AI discovered threat intelligence platforms can follow the darknet forums, code sharing sites, and others to know the future zero-day attack plans. This results in an organization being able to put measures in place before any threats surface and hence minimize their vulnerability to threats that have not been previously experienced.

## 7. Challenges and Limitations

### 7.1 False positives and alert fatigue

Another challenge that the use of AI has brought is with specific reference to false positives since the use of this technology has enhanced the detection of threats. Works that used highly sensitive machine learning models to detect the attacks can result in a high number of false alarms reducing the analysts' effectiveness due to alert fatigue. This problem is further compounded by complexities which defines today's IT environments and normal behaviors that can easily be mimicked by these schemes.

To this end, organisations are using multiple tier detection systems that involve the use of different AI tools in order to eliminate the issue of false positives. For instance, one of the stages in the system could be to incorporate an anomaly detection algorithm as the first level of filtering and then use the second level of classification to look at the possible threats in greater detail. Besides, there are frequent feedback mechanisms and an integration of active learning approaches to enhance the created models' accuracy.

The Ponemon Institute also conducted a survey that showed that security personnel spend an average of a quarter of their time identifying false positives; an area that could be made more effective through the proper use of AI (Ponemon Institute, 2020).

### 7.2 Adversarial AI and evasion techniques

Cybersecurity has transitioned to utilizing AI in the recent past, attacker are beginning to design complex methods to avoid detection by artificial intelligence systems. These malicious attacks on the AI-based systems entail a subversion of the features fed into an ML system. Common techniques include:

1. Evasion attacks: Download more powerful virus to detect and change its' payloads
2. Poisoning attacks: Another technique involved feeding the training sets with wrong information that would affect the working of the model.
3. Model stealing: Using resource models to work for new ways of evading detection

The scientists at the International Business Machines (IBM) created AI-based malware named DeepLocker to show what all the furore is about. DeepLocker employs deep neural networks to conceal the payload within it; the payload only executes when certain target conditions are achieved (Kirat et al. , 2018).

In response to these threats, cybersecurity is now aiming at building powerful AI models that cannot be easily attacked. Currently, methods of adversarial training, ensemble of models, and defensive distillation are being developed to increase model's defense.

### 7.3 Ethical considerations and bias in AI security systems

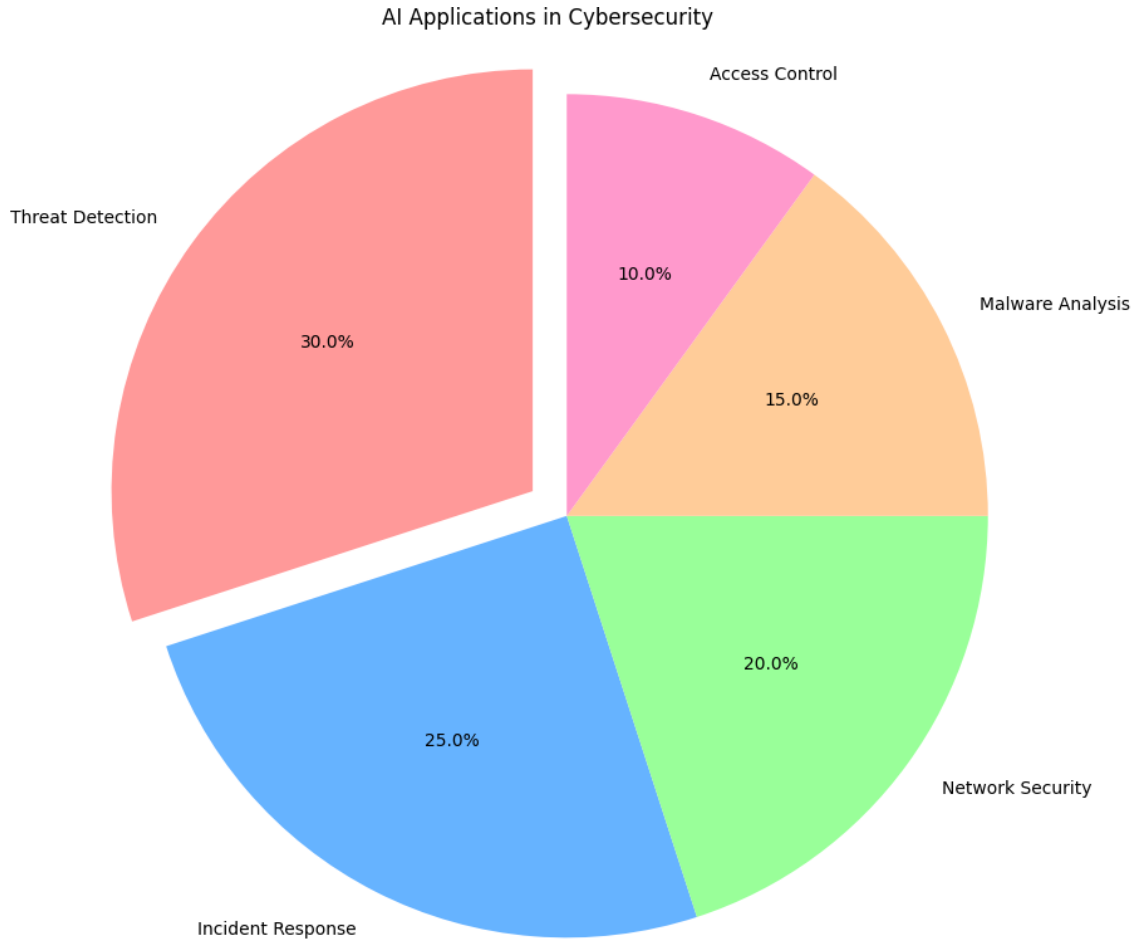
The employment of AI in cybersecurity has critical ramifications pertaining to ethics; these include privacy, transparency, and possible bias. Applications built into an AI system that monitor user action or traffic data may gather personal data, which can create issues on the data protection and data privacy and the GDPR regulation.

The AI models are also worth the problem of bias replication where the models are trained with certain bias, and therefore, deliver security decisions with the same bias. For instance, an ignorant AI system might be designed to categorise individuals within specific demographic segments as suspicious, even though they are not security threats.

To address these ethical challenges, organizations and researchers are focusing on:

1. Exploring the creation of robust explanation for AI models, so that one can easily understand why an optimum decision has been made.
2. Ensuring that the training data is of high quality and that it is fair in the way it treats patients.
3. A suggestion was made that organizations should carry out annual checks on the AI systems to determine places and areas that could have issues with bias.
4. The following is the set of guidelines towards the creation of ethical standards in the designing and utilization of artificial intelligence in cybersecurity.

The European Union has proposed the AI Act that regulates the actions of artificial intelligence and its applications deeming some of them as high risk such as cybersecurity AI application (European Commission, 2021).



## 8. Future Trends and Developments

### 8.1 Quantum computing and AI in cryptography

Quantum computing is the next big advancement in computer technology and it presents several threats and adaptations in the cybersecurity domain. Even though quantum computers pose a significant risk of being able to crack most of the presently used encryption techniques, they present the capabilities to improve the cryptographic frameworks as well. AI has a key function in the prospect of creating quantum-resistant cryptography and enhancing the quantum algorithms utilized in security.

Scientists have successfully implemented a quantum computer from the MIT and the University of Innsbruck utilizing Shor's algorithm whereby problem solving based on the factorization of large numbers is performed exponentially faster than on classical computers (Monz et al., 2016). This has brought out the need to come up with quantum resistant encryption solutions.

Applications of AI are being utilized in developing the concept and content of post quantum cryptographic systems. For instance, present-day advances in big data analytics are helping in enhancing the lattice-based cryptography, which is one of the methods of constructing quantum-safe encryption.

| Post-Quantum Scheme | AI Application |
|---|---|
| Lattice-based | Optimizing parameter selection, improving key generation efficiency |
| Hash-based | Enhancing tree traversal algorithms, optimizing signature sizes |
| Code-based | Improving decoding algorithms, enhancing key size reduction techniques |
| Multivariate | Optimizing public key generation, enhancing signature verification |

### 8.2 AI-enabled threat hunting and proactive defense

Another year the prospects of cybersecurity are shifting from the reactive approach focusing on the identification of threats and anomalies and towards more predictive and proactive methods that involve AI technology. The most sophisticated AI systems will form a system of constant surveillance of networks, and through the analysis of patterns will alert the user of possible threats before they can materialize. Another interesting area is the deployment of digital twins stimulated by artificial intelligence in the sphere of protection. These virtual copies of the IT infrastructures let the organisations replicate the attacks, try out the measures of protection, and fine-tune the security settings with minimal danger to the live systems. According to Gartner, by the year 2025 the projection is that approximately fifty percent of the large firms will use digital twins for enhancing the organizations' security (Gartner, 2022).

### 8.3 Integration of AI with other emerging technologies

As for the development of AI in cybersecurity, it will be simultaneously developed with other innovative scientific fields, which means that it will become more perfect, deeper, and the final product will be more comprehensive. Some key areas of integration include:

1. Internet of Things (IoT) security: AI will play the greatest role in protecting billions of connected devices enforcing Edge computing for the continuous detection and responding to threats in real-time.
2. 5G networks: With the advancement of 5G networks, AI will play a critical role in facilitating the complexity of the business organization's missions through networking and security of the network traffic.

3. Blockchain: The use of AI with block chain has benefits in areas of increased use of big data, secure exchange of information and decentralized threat detection systems.
4. Extended Reality (XR): Thus, AI will help accommodate VR and AR applications, providing protection for virtual spaces and ensuring the confidentiality of users' data.

## 9. Conclusion

### 9.1 Summary of key findings

As illustrated by this research, there has been a great revolution done by Artificial Intelligence in the sphere of cybersecurity. Machine learning and deep learning have greatly improved the levels of threat detection and have automated most of the incident response processes thereby improving the security position. Key findings include:

1. Another benefit of AI systems is the ability to take a large amount of data and process it in real time for more efficient threat identification.
2. Machine learning techniques have been reported to achieve great performance in realms including antivirus, traffic analysis, and users' behavioral analysis.
3. AI is very much applied in all dimensions of the incident response phase, bringing fewer response times and better resource use in security operations.
4. In the current world, complex artificial intelligence methods are being applied to prevent a particular kind of attacks which is zero-day threats and even find ways of preventing such types of attacks before they happen.

### 9.2 Implications for the future of cybersecurity

The security operations will gradually be more automatized, while AI will take over the simpler tasks as well as support the human analysts in more analytically complex decision-making. It will help security teams to upscale from the constant firefighting that results in a high number of alerts and incidents, to a position where they can work on advanced threat analysis and essential security projects. Cybersecurity professional's duties will change with increased focus on AI understanding and the capability to analyze AI and execute based on the data given. From this, it will be clear that organizations shall require to spend money on training their employees to enhance their know-how on the use of AI security tools and solutions. Eventually, as A I enroot itself into the cybersecurity, there should be improved interactivity and adaptability in how defence is done. The implemented AI technology would be smart systems that would forever be learning so that these organizations would be able to have an edge on the new threats more than they have ever been able to before. However, the above adaptation of AI increases new risks and with them comes new and unique ethical issue. Companies need to stay alert on the adversarial attacks and also need to ensure that the AI solutions are explainable, trustworthy, and devoid of any prejudice. The case suggests that the advanced framework of good governance of AI and the ethical standards in cyberspace will be determinative for the given issues.

### 9.3 Recommendations for further research

While AI has already made significant contributions to cybersecurity, there are several areas that warrant further research and development:

- Explainable AI for cybersecurity: That is why there is a tetrend towards more complex models, for which a request for the provision of clear explanations of decisions made is increasingly emerging. More work should be done to deepen the understanding of the explainable AI methodologies that are more suitable and applicable for various cybersecurity settings to make the use of AI in cybersecurity more trustworthy and effective to the extent of providing better cooperation between the AI systems and the analyst.
- Adversarial machine learning: The unrelenting nature of the gentleman and lady taunting each other in the realm of AI requires more studies on adversarial machine learning. This entails improving the AI models to be able to handle advanced evasion strategies and enhancing procedures of identifying and preventing adversarial attacks.

- AI-driven threat intelligence: Still, AI is even employed in threat intelligence, though there could be more sophisticated usage. Future work in the development of AI systems which could automatically create, verify, and share threat intelligence could greatly benefit the 'security industry' in threat response.
- Quantum-resistant AI algorithms: Thus, efforts have to be applied to finding AI algorithms that would still work without getting compromised by quantum computers' growth. This is especially elaborating new quantum-safe machine learning fundamentals and studying AI's potential significance in post-quantum cryptography.
- Ethical AI in cybersecurity: More work is required into how to define and implement properly normalised ethical guidelines for the use of AI for cybersecurity. This involves such as the issues of privacy, fairness and accountability where AI has taken over security.

Thus, it can be stated that the heavy investment in Artificial Intelligence in the cybersecurity context implies a shift in the paradigm of organizational cybersecurity measures. AI has found vast applicability in threat detection and response mechanisms; however, it has paved the way for new problem areas. Hence, further advancements are needed in the field of cybersecurity by implementing regular research and development to uncover AI capabilities at their best while dealing with their drawback and other concerns of moral principles. The path of development of cybersecurity will continue its future course based on the AI technology, and the organization that is able to adapt to and implement those technologies will be in a stronger position to combat the threats that are emerging in the modern business environment.

**References**

[1] AV-TEST. (2020). The best antivirus software for Windows Home Users. https://www.av-test.org/en/antivirus/home-windows/
[2] Ceja, C., et al. (2019). Deep learning for network intrusion detection. MIT Lincoln Laboratory. https://www.ll.mit.edu/news/deep-learning-network-intrusion-detection
[3] Darktrace. (2021). Autonomous Response: Threat Report 2021. https://www.darktrace.com/en/resources/wp-autonomous-response-2021.pdf
[4] European Commission. (2021). Proposal for a Regulation laying down harmonised rules on artificial intelligence. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence
[5] Gartner. (2021). Gartner Predicts 60% of Large Enterprises Will Implement Adaptive Access Control by 2025. https://www.gartner.com/en/newsroom/press-releases/2021-03-23-gartner-predicts-60--of-large-enterprises-will-implemen
[6] Gartner. (2022). Gartner Top Strategic Technology Trends for 2022. https://www.gartner.com/en/information-technology/insights/top-technology-trends
[7] Kirat, D., Jang, J., & Stoecklin, M. (2018). DeepLocker: Concealing Targeted Attacks with AI Locksmithing. BlackHat USA. https://i.blackhat.com/us-18/Thu-August-9/us-18-Kirat-DeepLocker-Concealing-Targeted-Attacks-with-AI-Locksmithing.pdf
[8] Microsoft Security Intelligence Report. (2021). https://www.microsoft.com/security/blog/2021/10/29/microsoft-digital-defense-report-2021/
[9] Monz, T., et al. (2016). Realization of a scalable Shor algorithm. Science, 351(6277), 1068-1070. https://science.sciencemag.org/content/351/6277/1068
[10] Morgan, S. (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[11] Palo Alto Networks. (2022). Next-Generation Firewall. https://www.paloaltonetworks.com/network-security/next-generation-firewall
[12] Phan, A., et al. (2021). Tinytection: Zero-Shot Learning for Deep Learning-Based Software Vulnerability Detection. Stanford University. https://arxiv.org/abs/2103.03851
[13] Ponemon Institute. (2019). The Cost of Cybercrime. https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

[14] Ponemon Institute. (2020). The State of Cybersecurity and Digital Trust 2020. https://www.accenture.com/us-en/insights/security/invest-cyber-resilience
[15] Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy. https://ieeexplore.ieee.org/document/5504793
[16] Veeramachaneni, K., et al. (2016). AI^2: Training a big data machine to defend. IEEE 2nd International Conference on Big Data Security on Cloud. https://ieeexplore.ieee.org/document/7502262