AI IN CYBER SECURITY

Prateeka Kalakonda[1], Jahnaavi Basa[2], J. P. Pramod3
[1,2]B.TechStudents Dept of Information Technology
Stanley College of Engineering and Technology for Women.
[3]Asst Professor, Dept of Physics Stanley College of Engineering and Technology for Women

ABSTRACT: AI has exponentially strengthened cyber security by continuous advancement of threat detection, prevention of malware, and enabling automated responses. It helps combat phishing, fraud, and zero-day vulnerabilities, while supporting cyber threat intelligence and identity management. Despite challenges like adversarial attacks and data privacy, AI is becoming a key tool for proactive and adaptive digital defense.

Key points:
Artificial Intelligence (AI), Automated Incident Response, Data Protection, Deep fake & AI-Enabled Attacks, Malware, Proactive Defense, Real-time Analytics, Threat Detection and Prevention

INTRODUCTION

The most trending and used term in our daily lives is AI. It became an essential par to four life. If you have used GPS, language translators, asking a questionto chatbot. Voila! You have come across AI. But what exactly is AI?

WHAT IS AI?

AI is an abbreviation of Artificial Intelligence. It is a combination of computer science and large sets of data that would allow AI to perform tasks that previously only humans could handle—like problem solving, understanding things, etc,.

With these distinctive properties, Ai is used in almost every field these days- mostly in Healthcare, Medicine, Education, Manufacturing and Industries and also in Security. This brings us to the topic, Cybersecurity

CYBER SECURITY

Cybersecurity is all about keeping our digital world safe. It protects computers, networks, and data from hackers, viruses, and other threats. It encompasses the technologies, processes, and controls designed to safeguard the confidentiality, integrity, and availability of information and the systems that process it.

Organizations and we individuals often face wide variety of cyber threats. Some of the common Cybersecurity threats are Malware: Malicious software (viruses, worms, Trojans, ransomware) designed to infiltrate, damage, or steal data from systems. Phishing: Deceptive tactics that trick users into revealing credentials. Ransomware: A form of malware that encrypts an organization's data and demands payment for its release, often coupled with data exfiltration threats. Denial-of-Service (DoS/DDoS) Attacks: Flooding networks or services with excessive traffic to render them unavailable to legitimate users.

Man-in-the-Middle (MitM) Attacks: Intercepting and potentially altering communications between two parties without their knowledge.

Insider Threats: Risks posed by individuals within an organization—whether through malicious intent or inadvertent actions—who have legitimate access to assets.

Deepfake & AI-Enabled Attacks: Using artificial intelligence to craft convincing fraudulent content (audio, video, or text) or to automate reconnaissance and attack generation.

Although AI can be exploited by attackers to create sophisticated malware and launch advanced cyber threats, it is equally powerful in defending against such attacks by enabling intelligent threat detection, automated incident response, and predictive security measures that strengthen overall cybersecurity. We have now run across Artificial Intelligence (AI), Cybersecurity and its threats. Now let us dive into the usage of AI in Cybersecurity.

WHY AI IN CYBERSECURITY?

AI is reshaping nearly every field and one among these fields is Cybersecurity. It altered Cybersecurity by bringing unmatched speed, precision, and adaptability.

The main difference comes when traditional security methods rely heavily on predefined rules, which often fail to recognize new or evolving attacks. AI, on the other hand, learns continuously from data. It analyzes millions of interactions in real time, identifying subtle anomalies that might indicate a potential breach.

AI IN CYBERSECURITY

As we get to know that AI analyzes large amount of data sets and algorithms and find accurate solutions. With these features, AI can reduce cyber threats and help enhance Cybersecurity.

METHODS OF ENHANCING CYBERSECURITY USING AI

1. Threat Detection and Prevention:

AI-driven systems excel at analyzing massive volumes of security data in real time to identify indicators of anomalous behavior that traditional signaturebased tools often miss. Traditional signature-based tools in cybersecurity are security systems that identify malicious threats with pre-defined signatures, that is, it matches against a database against of known attack signatures. AI can detect malware and phishing attempts with accuracy rates above 90%, compared to 30–60% for legacy signature-based systems.

A zero-day vulnerability is a previously unknown security flaw in software, hardware, or firmware that is unknown to the developer. The term "zero-day" indicates that defenders have had zero days to address or mitigate the vulnerability before it becomes exploited. Spot zero-day refers to the ability to detect and identify zero-day vulnerabilities and attacks before they can cause significant damage.

AI can spot zero-day exploits and advanced persistent threats (APTs) through pattern-recognition and anomaly-detection techniques that uncover subtle deviations from normal baselines.

AI can prioritize genuine alerts and reduce false positives—AI systems can cut the volume of irrelevant alerts by over 40%, freeing security teams to focus on true incidents.

2. Automated incident responses of AI:

AI in cybersecurity automates incident response by leveraging machine learning and artificial intelligence to rapidly detect, analyze, and mitigate threats in real time. This capability transforms traditional manual processes into faster, more efficient workflows, enabling quicker threat recognition, automated remediation actions, and continuous learning from security incidents.

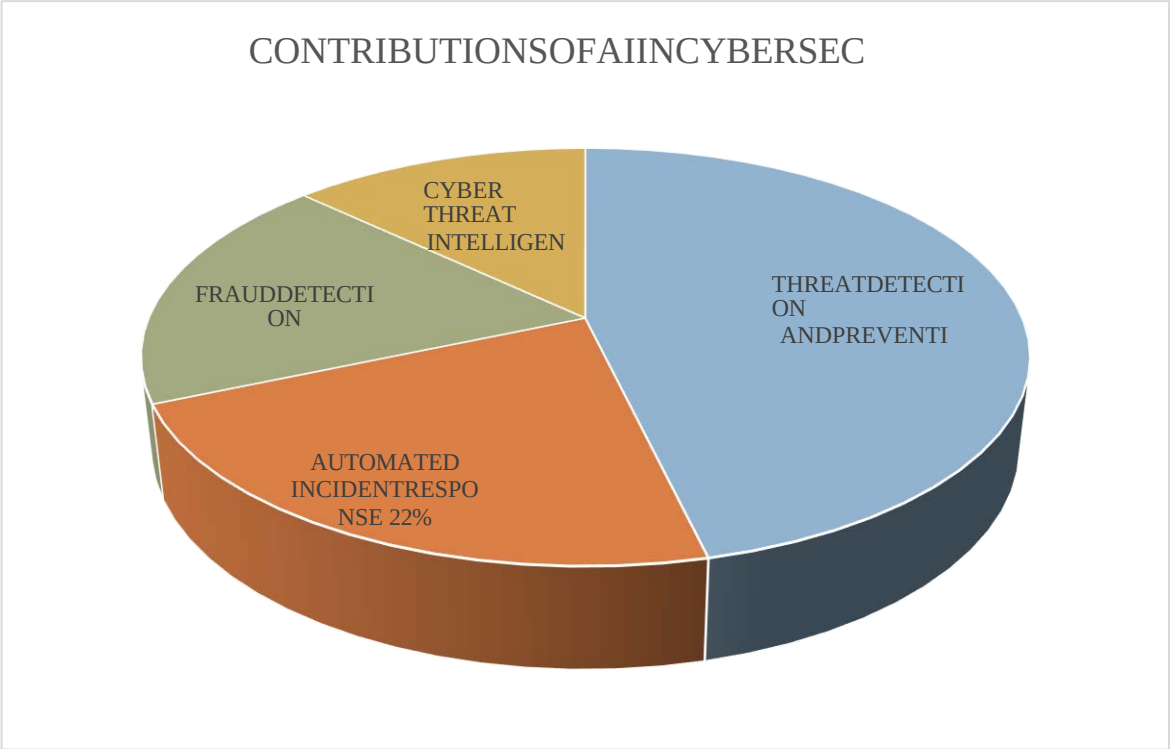
Key Features of AI-Powered Automated Incident Response:

Rapid Threat Recognition: AI systems analyze vast amounts of data from network traffic, system logs, and user behavior to identify anomalies and potential threats in real time. This reduces the time between attack initiation and discovery, enabling faster containment.

Automated Triage and Prioritization: AI automatically categorizes and ranks security alerts based on severity and potential impact, reducing false positives and helping security teams focus on the most critical incidents

3. Fraud Detection: Fraud detection using AI in cybersecurity is one of the most useful application where artificial intelligence helps organizations protect their financial information and data. Some useful ways where AI helps in Fraud Detection are 1. Pattern Recognition & Anomaly Detection: AI analyses normal user behavior (login times, device type). Any deviation (eg., sudden high-value purchase from a new location) is identified. Example: Detecting unusual credit card transactions. 2. Natural Language Processing (NLP): Detects fraud in emails, chats, or documents. Example: Spotting fake invoices or phishing attempts. 3. Behavioral Biometrics: AI analyzes typing speed, mouse movement, voice, or facial patterns. Helps detect if someone is impersonating an authorized user. 4. Deep Learning: Neural networks identify complex fraud schemes. Especially useful in catching fraud hidden within huge dataset analysis. (eg., banking) To sum up, these are the benefits of using AI in fraud detection: • Detects new and evolving fraud patterns faster than humans. • Reduces false positives (fewer genuine transactions wrongly flagged). • Provides real-time alerts. • Saves organizations from financial and reputational loss. 4. Cyber Threat Intelligence: Cyber Threat Intelligence (CTI) using Artificial Intelligence is a modern approach to identify, understand, and prevent cyberattacks. Traditional CTI relies on manual research and analysis to a great extent, which is often slow and unable to match with the speed of

evolving threats. AI solves this problem by automating the entire process of data collection, analysis, and prediction. It can scan through massive amounts of structured and unstructured data, even in dark web forums, to detect malicious activity. Through pattern recognition and machine learning, AI identifies unusual behavior that might signal a potential attack and can even predict new threats by studying past trends. Natural Language Processing (NLP) further enhances CTI by allowing AI to understand hacker communications, reports, and discussions that are not in standard data formats.



The use of AI also makes threat intelligence more efficient by prioritizing the most severe risks, ensuring that security teams focus on the most dangerous issues first. Another key advantage is the ability to generate real-time alerts, which helps organizations respond to threats instantly instead of after damage. Overall, AI-driven CTI transforms cybersecurity from a active process into a proactive defense system, giving organizations the ability to anticipate, prepare for, and block advanced and evolving cyber threats more effectively.

AI IN CYBERSECURITY: BEFORE Vs NOW

AI has dramatically transformed cybersecurity. Before AI, cybersecurity relied mostly on static rule-based systems and human interventions, but now it benefits from machine learning, real-time analytics, and independent incident response.

BEFORE:

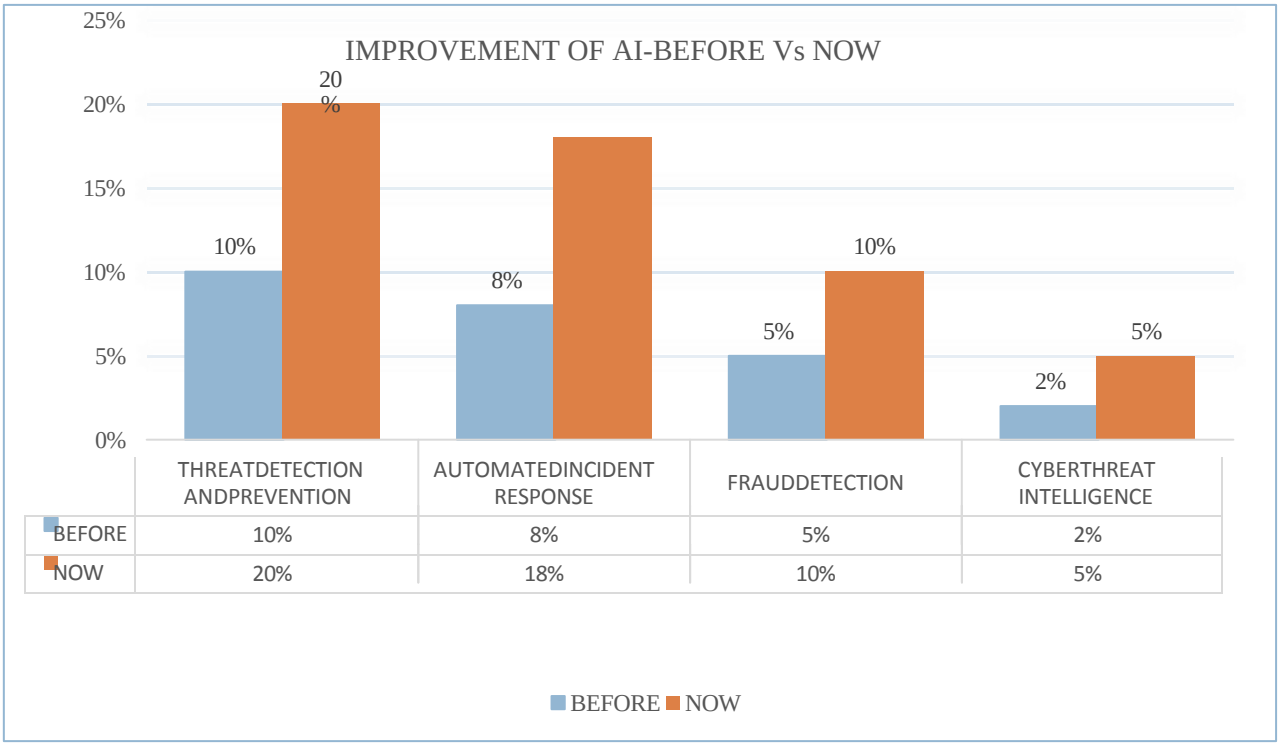
Before AI in Cybersecurity, Security systems depended on manually created rules and known signatures to recognize threats. New or sophisticated attacks bypassed these methods easily. Human analysts had to sift through large volumes of alerts, investigate incidents, and take improved steps, resulting in slow response times and increased operational burden.

Defenses also focused on known vulnerabilities and historical attack patterns, leaving organizations exposed to unknown and rapidly evolving threats. Most processes, from data classification to network segmentation and patching, required extensive human input and intervention.

NOW:

AI systems can now continuously learn from vast, evolving datasets—including network traffic, user behavior, and global threat intelligence—to detect anomalies and predict new threat patterns. Modern AI models no longer rely solely on known attack signatures—instead, they proactively search for deviations from established baselines, catching zero-days and emerging attack techniques.

Security operations are streamlined as repetitive, labor-intensive tasks (alert triage, sensitive data classification, threat hunting) become automated, freeing experts for strategic analysis. Lower False Alarms and Enhanced Accuracy: AI models adapt detection rules based on feedback and new data, vastly reducing false positive/negative rates compared to traditional methods. automation allows organizations to protect larger, more complex IT environments with less manual effort and lower long-term costs. Proactive Prevention & Future Readiness: AI-powered systems enable organizations to anticipate threats, harden defenses in advance, and maintain continuous improvement through learning cycle.



AI TECHNIQUE/ TECHNOLOGY	MAIN FUNCTION	EXAMPLE USE CASE	PRIMARY BENEFIT
Anomaly detection	Identifies unusual patterns in data	Spotting previously unknown malware	Detects zero-day and unknown threats
Machine learning-based Threat hunting	Proactively searches for hidden threats	Hunting persistent attackers in networks	Uncovers threats missed by automation
AI-driven threat intelligence	Correlates global and local signals	Real-time matching of emerging IoCs	Accelerates defense and adaptation
Deep learning for malware analysis	Inspects files/binaries for complex patterns	Identifying polymorphic or evasive malware	Improves detection accuracy
Automated Investigation	Gathers, correlates, and summarizes incident data	Generating detailed incident reports	Free analysts for desion-making

REVIEW OF LITERATURE

1. Enhancing Detection and Response Using Artificial Intelligence in Cybersecurity(2025): This article provides an analysis of how artificial intelligence is transforming cybersecurity within Security Operations Centers (SOCs). By highlighting applications such as ChatOps, DDoS mitigation, speech recognition, and image captioning, it demonstrates AI's capacity to process massive volumes of data, reduce false positives, and accelerate incident response. However, the paper also acknowledges inherent challenges, including technical limitations, ethical concerns, and privacy risks.

2. Artificial Intelligence in Cybersecurity: **A Comprehensive Review and Future Direction(2024):** This article views at the point how Artificial Intelligence (AI), especially Machine Learning (ML), is being used to improve cybersecurity. Since cybercrimes are becoming more advanced, AI helps by analyzinglargeamountsofsecuritydatatodetectpatterns,predictthreats,and respond automatically. The study is based on a detailed review of research papers collected from Scopus and Web of Science databases, starting withover 14,000 papers and narrowing down to 939 relevant ones. It high lights different applications of AI, such as anomaly detection and threat identification, while also discussing their effectiveness, challenges, and future trends in cyber security research.

3. Cybersecurity and Artificial Intelligence Applications: **A Bibliometric Analysis Based on Scopus Database(2023):** This article views on how the research on Cybersecurity and Artificial Intelligence (AI) has increased over the years and what areas are researchers are focusing on. It studies 501 papers from the Scopus database and finds that research activity has increased a lot since 2015. This shows that AI is becoming more important for protecting digital systems. It also points out the fact that many researchers and institutions are working together, creating a strong network that encourages collaboration.

Common research areas include network security, deep learning, and the Internet of Things (IoT). The article explains that AI can improve cybersecurity by making threat detection faster, automating defences, and reducing risks before they become serious problems.

4. 10 Benefits of Using AI for Cybersecurity(2022): This article talks about how AI these days is becoming essential for businesses to protect themselves from increasingly complex cyber threats like phishing, malware, and data breaches. With its ability to learn and improve over time, detect unknown threats, manage large amounts of data, and speed up threat detection and response, AI has become a powerful weapon for protection against hackers. AI can also handle repetitive security tasks efficiently, improve authentication methods, and help businesses make smarter security decisions. In this age where cybercrimes are increasing rapidly, using AI-based cybersecurity tools is no longer optional but necessary for businesses to stay safe and secure online.

5. Weaponized AI for cyber-attacks(2021): AI, which is often used to protect computer systems, is now being used to carry out cyberattacks. This article Explores real-world examples of faking data, like adversarial attacks on medical imaging and autonomous vehicles, some measures are suggested to reduce the impact of such attackers. These include improving the training of AI models with high-quality and secure data to make them less vulnerable to manipulation.

Developing systems that can detect fake or tampered inputs before they affect critical applications is also suggested. Using machine learning itself to identify and respond to attacks in real time is another important approach. This way, many cyberattacks can be dodged with efficiency.

6. The Impact of AI on Cybersecurity(2020): This article provides information of how AI is used to avoid data breach and other losses, AI was introduced into the field of cybersecurity. Replacing traditional security techniques with AI has increased threat detection rate to 95% but also brought up other issues. Hence, both AI and traditional methods have been combined. AI is efficient as it can handle multiple tasks and also reduce the cost of hardware, while saving time.

Companies can leverage AI to improve network security by learning network traffic patterns and recommending both functional grouping of workloads and security policy. Although AI can

improve security, it can also be exploited by cyber criminals so advancing AI such that it stays ahead of the fraudsters is essential.

RESULT ANALYSIS

Today, most companies are starting to use AI-powered tools, and studies show that more than half of IT teams already rely on AI in their daily security work.

This shows how quickly AI has moved from being an experimental idea to an essential part of modern defense. The use of AI in cybersecurity has increased the speed of security systems, making them easier to find both known and unknown threats compared to traditional rule-based methods.AI-powered threat detection can identify malware and phishing attempts with much higher accuracy Automated incident response systems enable reduction of threats and continuous security improvement, resulting in faster responses and reduced manual workload for professionals. AI-driven fraud detection solutions efficiently identify new and evolving threat patterns through behavioral analysis, anomaly detection, and deep learning methods. The application of AI to cyber threat intelligence provides proactive, real-time identification of advanced attacks, and delivers improved situational awareness. Compared to pre-AI approaches, modern AI systems have transformed cybersecurity from a reactive to a proactive, enabling organizations to prepare for, and block complicated attacks more effectively.

SUGGESTIONS

Training more cybersecurity professionals with AI/ML knowledge and also upskilling existing staff to understand both offensive and defensive AI capabilities would help in getting or providing new ideas for real time solutions. Preparing AI models to withstand adversarial attacks.

CONCLUSION

Artificial Intelligence (AI) has greatly improved the way organizations protect themselves from cyber threats. Artificial Intelligence and Cybersecurity both together, represent one of the most vital alliances in today's digital era. As technology advances, cybercriminals are also becoming more sophisticated, using AI itself to design advanced and hard-to-detect attacks. However, this dual nature of AI makes it equally powerful in strengthening defense systems. With its ability to analyze large amounts of data, detect anomalies in real time, automate responses, and predict evolving threats, AI transforms cybersecurity from a reactive approach into a proactive, intelligent, and adaptive shield.

In conclusion, the future of cybersecurity lies not in replacing human expertise,

but in enhancing it with AI's speed, accuracy, and adaptability. As cyber threats

continue to evolve, AI will remain an indispensable ally, enabling safer digital

environments and ensuring resilience in our interconnected world.

REFERENCES

1. Chris Gilbert , Mercy Abiola Gilbert , Maxwell Dorgbefu Jnr , Duah Jeremiah Leakpor , Kwitee D. Gaylah , Isaac A. Adetunde (2025) Enhancing Detection and Response Using Artificial Intelligence in Cybersecurity

2. Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction(10 DEC 2024)

3. O. S. Albahri, A. H. AlAmoodi (01 SEP 2023) Cybersecurity and Artificial Intelligence Applications: A Bibliometric Analysis Based on Scopus Database

4. Brijesh Kumar (June 7, 2022) 10 Benefits of Using AI for Cybersecurity

5. Muhammad Mudassar Yamin (2021) Weaponized AI for cyber attacks

6. Eddie Segal (2020) The Impact of AI on Cybersecurity

7.Victoria Shutenko (08 Aug 2024) AI in Cybersecurity: Exploring the Top 6 Use Cases

8.Orion Cassetto (18 Sep 2024) AI-Driven Incident Response: Definition and Components

9.BlinkOps Team (23 Oct 2024) AI for Incident Response: Benefits, Challenges & Best Practices

10.AI in incident response: Exploring use cases, solutions and benefits

11. AI-Powered Incident Response: Revolutionizing Threat Detection and Mitigation

12.The Role of Artificial Intelligence in Automated Incident Response