Detection and Prevention of Cyber Attack and Threat using AI

Krishna Arora
Department of Computer Science & Engineering, St. Andrews Institute of Technology & Management (SAITM)
Gurugram, Delhi NCR, India
krishna_249018@saitm.ac.in

Raj Bawane
Department of Computer Science & Engineering, St. Andrews Institute of Technology & Management (SAITM)
Gurugram, Delhi NCR, India
raj_249162@saitm.ac.in

Chetan Gupta
Department of Computer Science & Engineering, St. Andrews Institute of Technology & Management (SAITM)
Gurugram, Delhi NCR, India
chetan_249234@saitm.ac.in

Kahksha Ahmed
Department of Computer Science & Engineering, St. Andrews Institute of Technology & Management (SAITM)
Gurugram, Delhi NCR, India

Kahkasha.ahmed@gmail.com

Puneet Garg
Department of Computer Science & Engineering, KIET Group of institution, Delhi NCR, Ghaziabad, India
puneetgarg.research@gmail.com

***Abstract*—In the digital age, cybersecurity plays a crucial role in protecting personal and organizational data from evolving cyber threats. With increasing reliance on the internet for activities like online transactions, communication, and data storage, cyber-attacks have become more sophisticated, targeting both individuals and businesses. This paper explores the significance of cybersecurity in everyday life, focusing on various types of cyber-attacks such as phishing, malware, denial-of-service (DoS), and man-in-the-middle (MITM) attacks. Traditional security methods are no longer sufficient to combat these advanced threats, necessitating the integration of Artificial Intelligence (AI) in cybersecurity. AI-powered cybersecurity solutions leverage machine learning and deep learning algorithms to detect, prevent, and respond to cyber threats in real time. These techniques enhance threat detection by analyzing patterns, identifying anomalies, and predicting potential attacks before they occur. AI-driven tools, such as Intrusion Detection Systems (IDS), anomaly detection, and behavioral analysis, significantly improve cybersecurity measures by automating responses and reducing human intervention. This paper also highlights AI-based threat prevention strategies, including malware detection, phishing prevention, and intrusion prevention, which help secure networks, systems, and personal devices. While AI in cybersecurity presents challenges such as false positives and algorithmic transparency, its advantages in enhancing security resilience outweigh the limitations. As cyber threats continue to evolve, integrating AI-driven security solutions is essential for individuals and organizations to safeguard their digital assets and maintain data integrity in an increasingly interconnected world.**

Keywords*—Cybersecurity, AI, cybercrime, machine learning, Threat Detection, Fraud Detection

I. Introduction (*Heading 1*)

Cybersecurity has become a big global problem in today's linked digital landscape as cyber threats become more sophisticated. Cybercrime is quickly expanding, with attackers constantly refining their methods for exploiting weaknesses in systems, networks, and applications [1]. Traditional security solutions, such as firewalls, antivirus software, and rule-based intrusion detection systems, are no longer effective in protecting against modern cyber threats. Cyberattacks, such as ransomware, phishing, data breaches, and denial-of-service (DoS) attacks, affect both businesses and individuals, causing significant financial, operational, and reputational damage. As businesses' digital footprints grow and worldwide connectivity improves, protecting sensitive data and vital infrastructure from cyber threats has become a primary issue. With more than 70% of the world's population using the internet, there is a clear need for more advanced and adaptable cybersecurity solutions [2]. To solve these difficulties, artificial intelligence (AI) has emerged as a game-changing tool in the field of cybersecurity. AI-based cybersecurity (fig1) solutions take a proactive approach to threat identification, prevention, and response. Unlike traditional security systems, which rely on predefined signatures and rules, artificial intelligence (AI) can analyze massive volumes of data in real time, identifying trends, detecting abnormalities, and forecast future assaults. AI can recognize and respond to both known and undiscovered threats using machine learning (ML) and deep learning (DL) algorithms, making cybersecurity systems more resilient to emerging hazards [3].

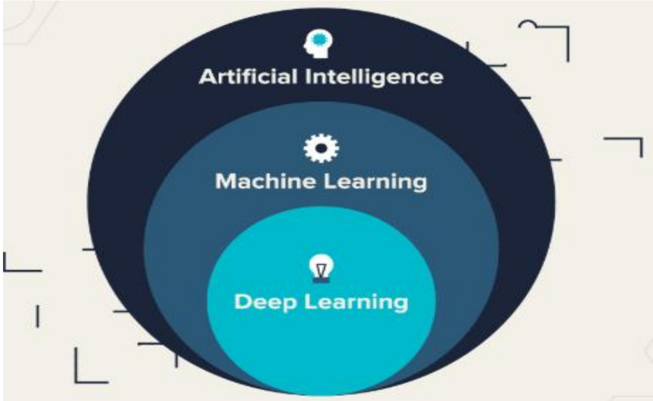

Fig. 1. AI-based cybersecurity

AI-powered security technologies continuously learn from previous occurrences and improve their detection skills, allowing enterprises to stay ahead of evolving cyber threats. Automation is one of the most significant advantages of AI in cybersecurity. AI-powered security systems can detect

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

and neutralize threats in real time, lowering response time and easing the pressure on human analysts. This is especially important in large-scale cyberattacks, where physical response may not be timely enough to avert damage.[4] AI also improves threat intelligence by gathering and analyzing cybersecurity data from many sources, allowing enterprises to gain actionable insights to increase their defense mechanisms. Furthermore, AI enhances authentication and access control by utilizing biometric identification, behavioral analysis, and anomaly detection to ensure that only authorized individuals have access to sensitive systems and information. Despite their advantages, AI-based cybersecurity solutions confront some problems [5].

One of the key issues is a lack of transparency, as AI algorithms frequently function as "black boxes," making it difficult to understand their decision-making processes. Furthermore, AI systems might produce false positives, causing unneeded alarms and increasing the effort for security professionals. Furthermore, hackers are using AI to develop more advanced attack techniques, necessitating ongoing improvements in AI-powered security systems. Overall, the incorporation of AI into cybersecurity is transforming how firms identify, prevent, and respond to cyber-attacks [6]. This paper mainly focuses on the various phases/aspects of cybersecurity different types of cyber-attacks, and the detection and prevention of threats and attacks. Also, we will look at the role of AI in cybersecurity, including its uses in threat detection and prevention.

II. Categories of Cyber Attacks

Cyber-attacks are categories in the following:

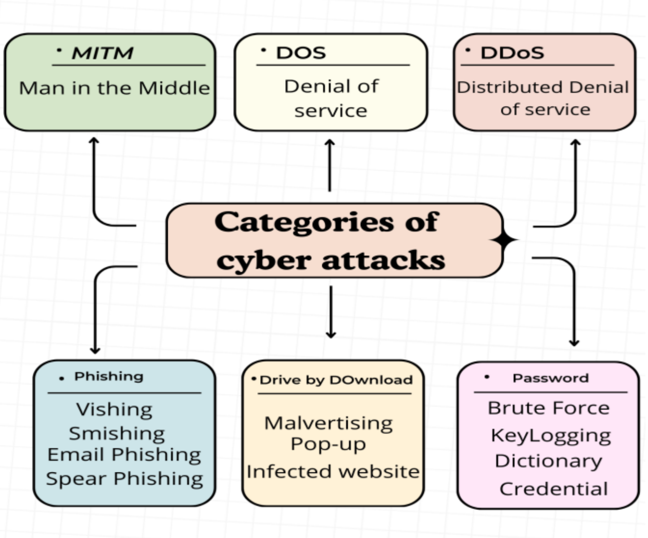

Fig. 2. Categories of Cyber Attacks

A. *Man-in-the-Middle (MITM) attack*

A Man-in-the-Middle (MITM) attack is a form of cyberattack in which an attacker secretly intercepts and modifies communication between two parties without them realizing it. An attacker places himself between the sender and receiver, intercepting or modifying the data in transit. This can result in data theft, financial scams, or unauthorized access to confidential information. MITM attacks are most often seen on unsecured or weakly secured networks, like public Wi-Fi. Attackers employ methods such as session hijacking, packet sniffing, and DNS spoofing to carry out the attack. Encryption (HTTPS, VPNs), multi-factor authentication, and secure connections can prevent MITM attacks. Examples of these are intercepting login credentials, money transactions, or sensitive emails. To counter these attacks, the users must shun public Wi-Fi, ensure SSL certificates, and implement stringent security protocols during browsing [7].

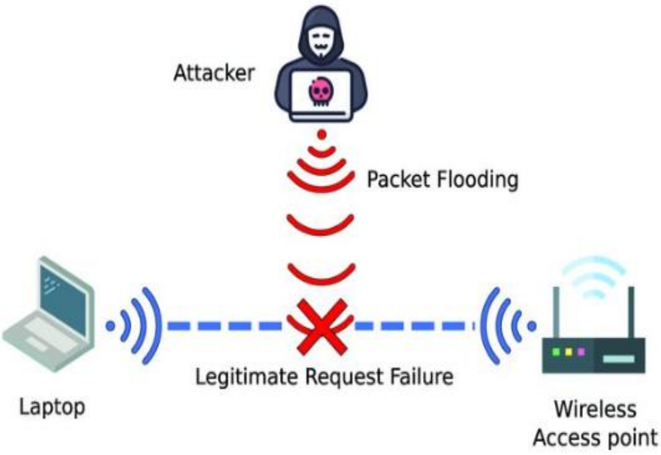

Fig. 3. Man-in-the-Middle (MITM) attack

B. *DoS (Denial of Service) attack*

A DoS (Denial of Service) attack is an online attack where a system, network, or server is overwhelmed with too many requests by an attacker, rendering it slow or even unusable to normal users. It is often executed from a single network connection or device [8]

C. *DDoS (Distributed Denial of Service) attack*

A DDoS (Distributed Denial of Service) attack is an upgraded version, where several hijacked devices (botnets) are employed to overwhelm a target with traffic, and it becomes more difficult to halt. Attackers utilize techniques such as UDP floods, SYN floods, and HTTP request floods to interfere with services. [9] To block DoS/DDoS attacks, organizations employ firewalls, load balancers, rate limiting, and DDoS protection services. Evading dubious downloads and updating security systems can also guard against such attacks.

D. *Phishing attack*

A phishing attack is a form of cybercrime in which cyber attackers deceive individuals into exposing sensitive information such as usernames, passwords, or financial information by impersonating a reliable organization. It is often conducted through fake messages, websites, or emails that appear genuine but are meant to steal information. Typical phishing tactics involve email phishing, spear phishing (sophisticated attacks), vishing (voice phish), and smishing (SMS phish) [10]. Attackers use urgency like fictitious security notices or winning opportunities to deceive victims into downloading malware or clicking harmful links.To guard against phishing, users must check the senders of emails, not click on unfamiliar links, turn on multi-factor authentication (MFA), and install security software. Organizations can also implement awareness training to inform employees about phishing threats.

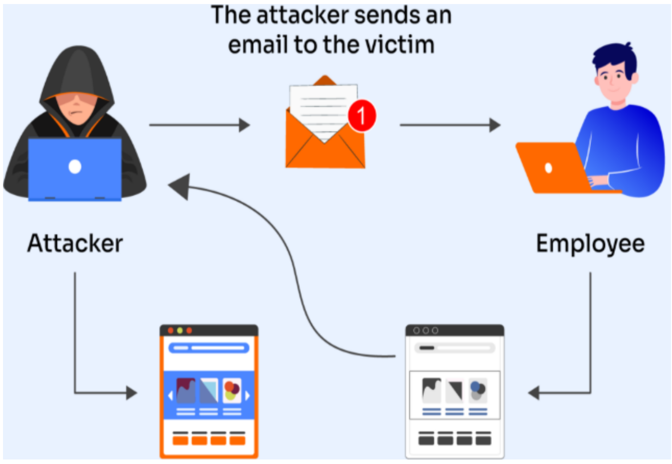

Fig. 4. Phishing attack

E. Drive-by Download attack

A Drive-by Download attack happens when a user inadvertently downloads malicious software simply by visiting an infected website, looking at an infected ad, or clicking on a misleading pop-up. In contrast to standard malware downloads, this attack does not involve the user deliberately downloading a file—it occurs quietly in the background. Attackers use vulnerabilities in browsers, plugins, or older software to install malware, which may steal information, hijack a system, or install ransomware. Sources typically include malicious advertisements (malvertising), imposter updates, and infected websites. [11] To guard against drive-by downloads, users must update software, employ a robust antivirus, turn off unnecessary browser plugins, and steer clear of suspicious links or advertisements. Organizations can also implement web filtering and endpoint security solutions to reduce risks.

F. Password attack

A password attack is a computer threat in which attackers try to gain unauthorized access to accounts or systems by cracking or stealing passwords. These attacks can be performed using different methods, including:[12]

1) Brute Force Attack

Attempting all possible combinations of passwords until the right one is discovered.

2) Dictionary Attack

Employing a list of common passwords or words to guess the right password.

3) Credential Stuffing

Employing leaked username-password pairs from previous data breaches.

4) Keylogging

Logging keystrokes by malware to acquire passwords.

5) Phishing

Bait users to expose their passwords with spurious emails or sites.

G. AI-based security framework

The suggested paradigm, Cyber Security in Financial Sector Management (CS-FSM), uses artificial intelligence to analyze all incursions and allows users to identify whether they are safe. Otherwise, it prevents the entry and alerts the control room or accessing personnel. Figure 3 depicts the overall systematics of the proposed system. All of the clients' financial information, banking sector, and other data are saved in a database protected by cyber security. When a single person, client, or threat attempts to gain access to that data, the firewall prevents it from happening. Genuine entries are permitted to store the data. These data are encrypted with either a private key or a public key.

Once encrypted, they will be stored in a database, ensuring that the data is safe from hackers. Using the KNN algorithm, artificial intelligence creates the best prediction model for both trusted and untrusted inputs. This algorithm creates a model based on the data provided by authorized individuals. After developing an effective prediction model, information access is rigorously tested. If an unknown entry or a virus attempts to use the information stored in the database, the prediction model will examine it, prevent further entrance, and notify the authorized person. This proposed model ensures the safety of financial data.

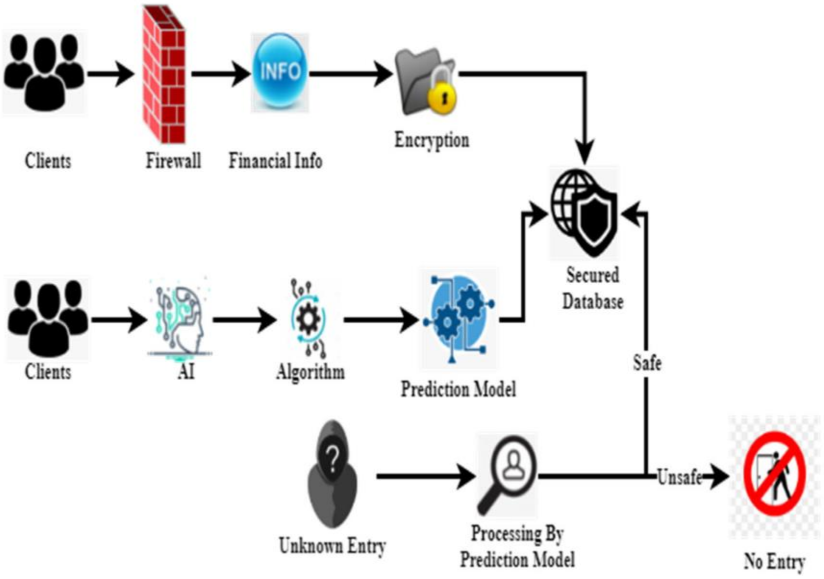

Fig. 5. AI based security framework used in security system

Artificial intelligence can be used to analyze the default risk of consumer and microenterprise loan candidates. The platform analyzes investment data and algorithms to find patterns and evaluate which applications are good or bad. Predictive analytics can aid in the detection of fraudulent behavior by analyzing the most effective operational procedures for transactions, sales, and transactions. Patterns can be detected by examining both structured and unstructured data (emails, reviews, and forum postings). The techniques utilized for prediction include the Enhanced Encryption Standard and K-Nearest Neighbor. Financial institutions should reassess their current back-office and front-end tools and procedures for protecting information as it moves throughout the company. They should include additional verification levels and security mechanisms with tiered checks to ensure secure transactions across several channels. Banking security is a critical concern in this day and age. One of the topics to keep in mind is the cybersecurity danger. These security flaws lead to fraud and other illegal activities. Every year, more and more people become victims of bank fraud. Financial safety net initiatives aim to reduce the frequency and severity of credit crises, which have economic effects. Whether corporate or state-sponsored, the threat financing industry usually associates parties without expenses [12]

III. Artificial Intelligence Techniques in Cyber Security

AI approaches have transformed the realm of cybersecurity. These are the approaches used by cybersecurity specialists to evaluate massive amounts of data, uncover abnormalities and trends, and identify possible risks before they become attacks.

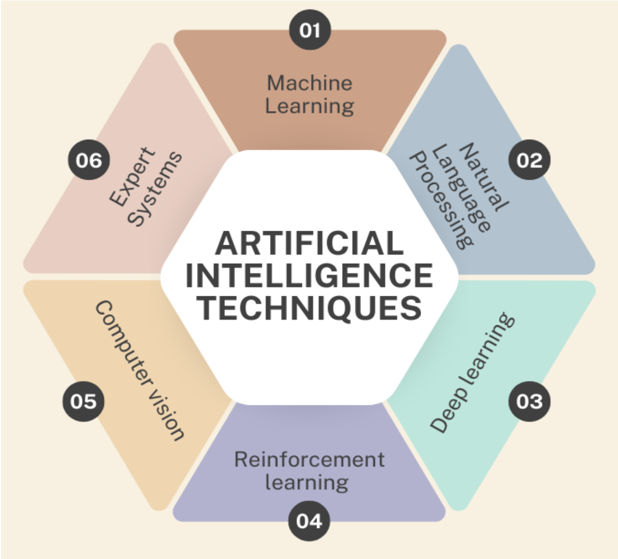

Fig. 6. Artificial intelligence techniques in cyber security

The common AI techniques used in cybersecurity are following:

A. *Machine Learning:*

It is a sort of artificial intelligence in which systems may learn from data without being explicitly programmed. Machine Learning algorithms use massive datasets of both benign and malicious traffic to uncover patterns and identify potential threats. Malware detection, network intrusion detection, and anomaly detection are all examples of activities that involve machine learning [13].

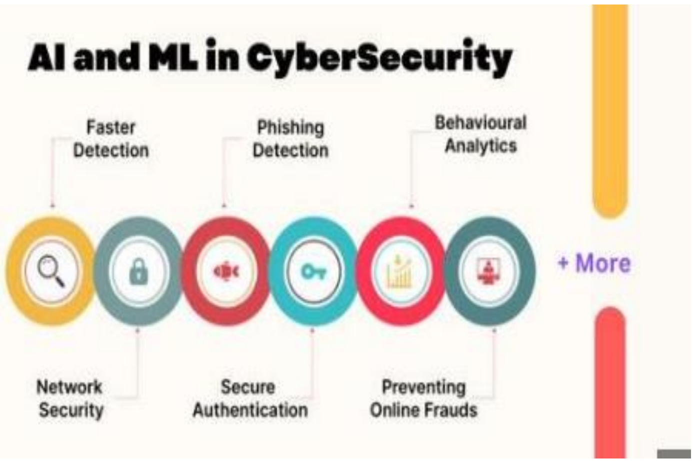

Fig. 7. AI and ML in cybersecurity

B. Natural Language Processing

It is a sort of artificial intelligence in which computers can read and interpret human language. In cybersecurity, natural language processing (NLP) is used to identify possible vulnerabilities in unstructured data sources such as social media feeds and online forums.

C. Deep learning

Deep neural networks are used in this area of machine learning to extract complicated patterns from data. It is used in cybersecurity for detecting malware, phishing, and fraud.

D. Reinforcement learning

It is a subset of ML that focuses on judgment. Reinforcement learning can educate cybersecurity systems to respond appropriately to attacks based on the situation and perceived threat level.

E. Computer vision

This AI method helps computers interpret and evaluate visual data. Its applications in cybersecurity include facial recognition and video surveillance.

F. Expert Systems

These AI systems replicate human experts' decision-making abilities in a specific domain. These systems are used in cybersecurity to detect and respond to intrusions and identify vulnerabilities.

IV. Threat Detection using AI

Artificial intelligence-based threat detection techniques are extensively applied across cybersecurity, anti-fraud, and physical security. These techniques utilize machine learning, deep learning, and statistical analysis to detect threats in real time. The following are some of the prominent AI-based threat detection techniques: [14]

A. Network Security Threat Detection

AI-powered Intrusion Detection Systems (IDS) monitor network traffic for anomalies, such as unauthorized access or unusual login attempts. Behavioral analysis helps detect deviations from normal user activity, identifying potential insider threats. Security Information and Event Management (SIEM) systems, enhanced with AI, analyze log data in real time to detect security incidents [15]. AI-based anomaly detection improves cybersecurity by identifying threats proactively, reducing false positives, and automating responses to mitigate attacks before they escalate.

B. Malware Detection

AI enhances malware detection by combining signature-based detection with behavioral analysis. Heuristic analysis allows AI to identify previously unknown malware based on suspicious activities. AI-powered sandboxing runs files in a virtual environment, observing their behavior before execution. Advanced deep learning models can recognize hidden threats by analyzing patterns across large datasets. These techniques enable AI to detect polymorphic malware, zero-day attacks, and evolving threats more efficiently than traditional rule-based security systems.

C. Email & Phishing Detection

AI-powered Natural Language Processing (NLP) scans email content for phishing attempts by detecting malicious links, misleading language, and suspicious requests. Image recognition helps identify fake logos and altered brand elements used in phishing emails. AI also employs anomaly detection to analyze sender behavior, flagging deviations from normal communication patterns. By integrating these techniques, AI reduces the risk of social engineering attacks, helping users and organizations avoid financial loss and data breaches.

D. Fraud Detection

AI-powered fraud detection analyzes vast amounts of financial data to identify fraudulent transactions. Credit card fraud prevention uses AI to detect suspicious spending patterns. Anomaly-based detection identifies unusual behaviors like multiple failed login attempts or unexpected geographic access. AI-powered identity verification uses facial recognition and biometric analysis to prevent identity theft. By leveraging real-time data processing and pattern recognition, AI enhances security in banking, e-commerce, and online payment platforms.

E. Endpoint Security

AI-driven endpoint security solutions protect devices from malware, ransomware, and unauthorized access. AI-powered antivirus software uses deep learning to identify new threats based on behavior rather than known signatures. User and Entity Behavior Analytics (UEBA) detects insider threats by monitoring unusual activity on endpoints. AI enhances ransomware detection by recognizing encryption-based attacks in real time, stopping them before they encrypt critical files. These systems provide proactive defense against evolving cyber threats.

F. Physical Security Threat Detection

AI enhances physical security through facial recognition, object detection, and crowd behavior analysis. AI-driven biometric security systems prevent unauthorized access by verifying identities. Object detection models identify weapons or suspicious items in surveillance footage. AI-powered crowd analytics assess abnormal behavior in large gatherings to detect potential security threats. By integrating real-time monitoring and automated alerts, AI strengthens public safety, corporate security, and law enforcement efforts.

G. IoT Security

AI enhances IoT security by detecting anomalous device behavior, preventing cyber-attacks on smart devices. AI-driven anomaly detection monitors IoT traffic to flag unusual activity. Botnet detection identifies and mitigates large-scale automated attacks, such as DDoS attacks. AI-based smart authentication improves security for connected devices by enabling biometric authentication and behavior-based access control. These techniques help secure smart homes, industrial IoT, and healthcare devices from cyber threats.

H. AI in Threat Intelligence

AI-driven threat intelligence automates cyber threat hunting by analyzing security logs, network data, and dark web activity [15]. Cyber Threat Intelligence (CTI) aggregates real-time data to predict and prevent attacks. Predictive analytics helps forecast potential threats based on historical attack patterns. AI-powered systems enhance cybersecurity by identifying vulnerabilities before they are exploited, improving response times, and reducing human effort in manual threat analysis. These capabilities strengthen proactive security measures across industries.

V. Threat Prevention Using AI:

AI can be used to detect and prevent threats. AI-powered systems can recognize possible dangers and take proactive steps to keep them from causing harm. Here are some instances of how AI is used to counter threats:

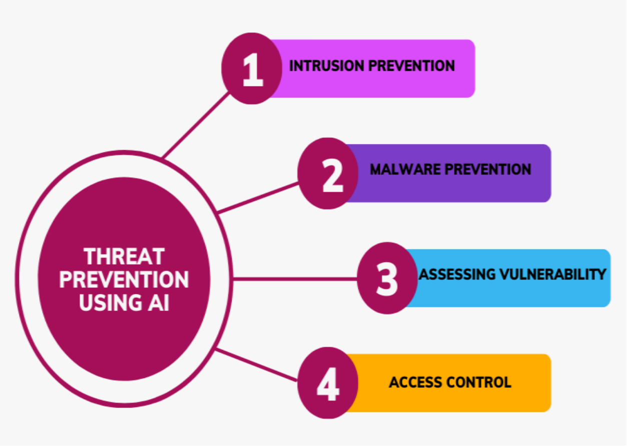

Fig. 8. Threat prevention using AI

A. Intrusion Prevention

Artificial intelligence-based Intrusion Prevention Systems (IPS) are crucial in detecting and blocking potential cyber intrusions before they reach a network. Traditional intrusion detection systems use predefined rules and signature-based detection, which are frequently unsuccessful against zero-day assaults and advanced persistent threats (APTs) [16]. AI-powered intrusion prevention systems use machine learning (ML) and behavioral analysis to detect suspicious activity, even if it does not follow known attack patterns. These systems continuously monitor network traffic, detect irregularities, and respond quickly, such as banning malicious IP addresses, flagging suspicious users, or isolating infected devices. AI-based IPS solutions use real-time threat intelligence to predict and eliminate cyber-attacks before they cause harm, maintaining network security and integrity.

B. Malware Prevention

AI-based antimalware solutions provide improved protection against dangerous software such as viruses, ransomware, Trojans, and spyware. Unlike traditional antivirus software, which depends on signature-based detection, AI-driven malware prevention solutions examine file activity, code structure, and execution patterns to detect possible threats before they are executed. Deep learning and heuristic analysis enable AI to detect and block new and evolving malware that traditional systems may miss. AI-powered sandboxing techniques execute questionable files in a controlled environment to assess their behavior before granting them access to the system. Additionally, AI can automate malware classification, giving cybersecurity professionals with faster and more accurate insights to effectively reduce risks.

C. Phishing Prevention

Phishing is one of the most prevalent and effective cyber-attack strategies, in which attackers trick users into disclosing sensitive information such as login credentials and financial information. AI-powered anti-phishing systems can detect and prevent phishing attacks by evaluating email content, sender activity, and embedded links in real time. These systems use Natural Language Processing (NLP) to detect suspect language patterns, unusual demands, and social engineering strategies in emails. AI also evaluates URL structures and compares them to known phishing databases to identify bogus websites that steal user data. Organizations may greatly minimize the risk of cyber events caused by phishing by integrating AI-driven phishing protection into email security platforms and web browsers [17]

D. Vulnerability Assessment

AI-based vulnerability assessment solutions assist enterprises in identifying and addressing potential security flaws in their networks, apps, and devices. Traditional vulnerability scanners sometimes rely on predefined vulnerability databases, which can quickly become outdated. AI-powered systems, on the other hand, continuously analyze network traffic, system configurations, and user behaviors in order to detect previously unknown weaknesses and emerging threats. These systems use predictive analytics to evaluate risk and prioritize vulnerabilities based on their potential impact. AI may also simulate cyberattacks to assess system defenses and provide automatic security fixes or mitigation techniques. By proactively correcting vulnerabilities, organizations may limit their attack surface and keep hackers from exploiting security flaws.

E. Access Control

AI-powered access control solutions increase security by dynamically regulating user rights and preventing illegal access to sensitive data and key systems. Traditional access control approaches rely on static rules that may fail to detect insider threats or compromised credentials [18]. To determine the legality of access requests, AI-powered access control solutions employ biometric identification, behavioral analytics, and contextual information. To detect anomalies, these systems assess data such as user location, device type, login history, and real-time behavior. If an odd access attempt is identified (for example, an employee checking in from an unfamiliar country), AI can initiate further authentication procedures or deny access outright. AI-powered access control also combines with zero-trust security models, guaranteeing that users and devices must continually authenticate their identities before accessing resources.

VI. Phishing website threat detection through machine learning algorithms

Here mentioned the some example of phishing website threat detection using machine learning algorithms

According to Basit et al. (2021), phishing attacks have become a major cybersecurity issue, targeting individuals, governments, and corporations by stealing critical data via faked websites and emails. Their research reviews the literature on several AI-based detection strategies, such as machine learning, deep learning, hybrid learning, and scenario-based approaches. It examines various research on phishing detection, outlining their merits and weaknesses. Furthermore, the study examines existing issues in phishing detection and proposes future research topics to better security against such assaults [19]

According to Kahksha et al. (2019), as phishing attempts increase alongside the growth of e-commerce, forecasting and blocking such risks is critical for protecting online transactions. Artificial intelligence algorithms enable the rapid and accurate processing of large amounts of data, making them useful for phishing detection. Their study uses machine learning algorithms—Random Forest, Decision Tree, Neural Networks, and Linear Models—to identify websites as phishing, suspicious, or authentic based on distinctive criteria. By automating this classification, consumers are protected without having to manually verify each site. The study examines the effectiveness of different algorithms in terms of accuracy, error rate, precision, and recall to create an effective phishing detection model [20].

VII. Conclusion

Artificial intelligence (AI) is becoming increasingly important in cybersecurity, providing enhanced solutions beyond standard threat detection methods. AI-powered systems use machine learning, deep learning, natural language processing, predictive analytics, and behavioral analytics to analyze large volumes of data, discover patterns, and predict cyber risks. These systems improve security by identifying both known and unknown threats while also being useful for access control, vulnerability assessment, intrusion prevention, malware protection, and phishing detection. As technology advances, AI's role in cybersecurity will increase, making it critical for businesses to implement these solutions to protect their systems from intrusions.

References

[1] Gupta, S., & Garg, P. (2021). An insight review on multimedia forensics technology. Cyber Crime and Forensic Computing: Modern Principles, Practices, and Algorithms, 11, 27. DOI: 10.1515/9783110677478

[2] Shrivastava, P., Agarwal, P., Sharma, K., & Garg, P. (2021). Data leakage detection in Wi-Fi networks. Cyber Crime and Forensic Computing: Modern Principles, Practices, and Algorithms, 11, 215. https://doi.org/10.1515/9783110677478-010

[3] Yadav, P. S., Khan, S., Singh, Y. V., Garg, P., & Singh, R. S. (2022). A Lightweight Deep Learning-Based Approach for Jazz Music Generation in MIDI Format. Computational Intelligence and Neuroscience, 2022. DOI:10.1155/2022/2140895

[4] Gupta, M., Garg, P., & Agarwal, P. (2021). Ant Colony Optimization Technique in Soft Computational Data Research for NP-Hard Problems. In Artificial Intelligence for a Sustainable Industry 4.0 (pp. 197-211). Springer, Cham. https://doi.org/10.1007/978-3-030-77070-9_12

[5] Malik, M., Garg, P., & Malik, C. (2024). Artificial intelligence-based prediction of health risks among women during menopause. Artificial Intelligence and Machine Learning for Women’s Health Issues, 137-150. https://doi.org/10.1016/B978-0-443-21889-7.00010-5

[6] Meenakshi, P. G., & Shrivastava, P. (2021). Machine learning for mobile malware analysis. Cyber Crime and Forensic Computing: Modern Principles, Practices, and Algorithms, 11, 151. https://doi.org/10.1515/9783110677478-008

[7] Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. IEEE communications surveys & tutorials, 18(3), 2027-2051.

[8] Gu, Q., & Liu, P. (2007). Denial of service attacks. Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications, 3, 454-468.

[9] Salim, M. M., Rathore, S., & Park, J. H. (2020). Distributed denial of service attacks and its defenses in IoT: a survey. The Journal of Supercomputing, 76, 5320-5363.

[10] Ahmed, K., & Naaz, S. (2019, February). Detection of phishing ebsites using machine learning approach. In Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India.

[11] Cova, M., Kruegel, C., & Vigna, G. (2010, April). Detection and analysis of drive-by-download attacks and malicious JavaScript code. In Proceedings of the 19th international conference on World wide web (pp. 281-290).

[12] Mishra, S. (2023). Exploring the impact of AI-based cyber security financial sector management. Applied Sciences, 13(10), 5875.

[13] [13]Raza, M., Iqbal, M., Sharif, M., & Haider, W. (2012). A survey of password attacks and comparative analysis on methods for secure authentication. World applied sciences journal, 19(4), 439-444.

[14] Garg, P. (2024). Prediction of female pregnancy complication using artificial intelligence. In Artificial Intelligence and Machine Learning for Women’s Health Issues (pp. 17-35). Academic Press. https://doi.org/10.1016/B978-0-443-21889-7.00001-4

[15] Khanna, A., Rani, P., Garg, P., Singh, P. K., & Khamparia, A. (2021). An Enhanced Crow Search Inspired Feature Selection Technique for Intrusion Detection Based Wireless Network System. Wireless Personal Communications, 1-18. https://doi.org/10.1007/s11277-021-09144-1

[16] Lee, J., Kim, J., Kim, I., & Han, K. (2019). Cyber threat detection based on artificial neural networks using event profiles. Ieee Access, 7, 165607-165626.

[17] Gupta, S., & Garg, P. (2023). Code-based post-quantum cryptographic technique: digital signature. Quantum-Safe Cryptography Algorithms and Approaches: Impacts of Quantum Computing on Cybersecurity, 193. https://doi.org/10.1515/9783110798159-014

[18] Samarati, P., & De Vimercati, S. C. (2000). Access control: Policies, models, and mechanisms. In International school on foundations of security analysis and design (pp. 137-196). Berlin, Heidelberg: Springer Berlin Heidelberg.

[19] Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommunication Systems, 76, 139-154.

[20] Ahmed, K., & Naaz, S. (2019, February). Detection of phishing websites using machine learning approach. In Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India.