Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

AI and ML Driven Cyber security: Emerging Technologies and Future Perspectives

[1]Dr.M.Kundalakesi,[2]Harnisya Siva,[3]AbrahamS

[1]AssistantProfessor,[2,3]Students of BCA, Department of Computer Application, Sri Krishna Arts and Science College,

Coimbatore.

ABSTRACT:

The rapid development of digital technologies and the increasing dependence on connectedsystemshavegreatlyincreasedtheriskof cybersecuritythreats.Organizations and individualsarefacingvariouscyber-attackssuchasmalware,phishing,ransomware,denialof-service attacks, and advanced persistent threats. These attacks are becoming more complex, frequent,anddifficulttodetectusingtraditionalsecuritymethods.Conventionalcybersecurity solutions mainly depend on predefined rules and signature-based detection, which are often ineffective against new and unknown threats. To overcome these challenges, Artificial Intelligence(AI)andMachineLearning(ML)havebecomeimportanttechnologiesinmodern cyber security. Artificial Intelligence enables machines to perform tasks that require human intelligence, including learning, reasoning, and decision-making.

MachineLearningallowscomputersystemstolearnfromdata,identifypatterns,andimprove their performance without requiring direct programming. In cyber security, AI and ML techniques help analyzelargeamounts of network traffic, systemrecords, and user behaviour datainrealtime.Thesetechnologiessupportthreatdetection,intrusionidentification,malware classification, anomaly detection, and prediction of possible cyber-attacks. Different learning methods such as supervised learning, unsupervised learning, and reinforcement learning are used to identify existing threats and discover new attack patterns.AI-based cyber security systems improve detection accuracy, reduce false alarms, and provide faster responses to security incidents.

MachineLearning-basedIntrusionDetectionSystems(IDS)andIntrusionPreventionSystems (IPS) can identify complex attack behaviours that may not be detected by traditional approaches. AI also helps automate incident response by reducing human dependency and improving response speed. Behaviour analysis using ML further strengthens security by identifying unusual user activities and possible insider threats.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

INTRODUCTION:

The increasing use of digital platforms, cloud computing, mobile devices, and interconnected networks has completely changed the way organizations and individuals manage information. Although digital transformation provides better communication, efficiency, and accessibility, it has also introduced several cyber security challenges. Cyber threatssuchasmalwareattacks,phishing,ransomware,unauthorizedaccess,anddatabreaches are continuously increasing in both number and complexity.Traditional security mechanisms basedonfixedrules,signatures,andmanualanalysisarenolongersufficienttoprotectmodern digitalenvironments.ArtificialIntelligence(AI)andMachineLearning(ML)haveemergedas effective solutions for improving cyber security systems.

AIreferstotheabilityofmachinestoperformintelligentactivitiessimilartohumanthinking, while ML focuses on developing algorithms that learn from previous data and improve their decision-making ability. The application of AI and ML in cyber security allows systems to processlargevolumesofinformationgeneratedfromnetworks,applications,andusers.These technologies can detect abnormal patterns, identify malicious activities, and predict possible security threats before serious damage occurs. Machine learning models are capable of recognizing known attack patterns as well as identifying previously unknown threats. This makes them highly useful for detecting zero-day attacks and advanced cyber threats that can bypass traditional security tools.

AI-based cyber security solutions are widely used in intrusion detection, malware analysis, frauddetection,vulnerabilityassessment,andautomatedincidentresponse.Theyhelpsecurity teams by reducing manual workload, improving threat identification, and enabling faster decision-making. Despite these advantages,AI and MLimplementation also faces challenges includingdataavailability,privacyconcerns,lackoftransparencyindecision-making,andthe possibility of attacks against AI models.

However,continuousimprovementsintechnologyarehelpingovercometheselimitations.The integration of AI and ML into cyber security provides a powerful approach for developing intelligent, adaptive, and reliable defence systems.As cyber threats continue to evolve, these technologies will become increasingly important for protecting digital information and infrastructure.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

AIAND MLTECHNIQUESUSEDIN CYBERSECURITY:

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

Artificial Intelligence and Machine Learning techniques play an important role in improving cyber security by providing automated, intelligent, and adaptive solutions. These methods help organizations detect threats, analyze attacks, and respond effectively.

1. SupervisedLearning:

Supervisedlearninguseslabelleddatasetswheremodelsaretrainedusingexamplesofnormal and malicious activities.These algorithms are commonly used for classification tasks such as malware detection, spam filtering, and intrusion detection.

Commonsupervisedlearningalgorithmsinclude:

- DecisionTree
- RandomForest
- SupportVectorMachine(SVM)
- NaïveBayes
- LogisticRegression

These models identify patterns from previous attacks and classify new activities as safe or harmful.

2. UnsupervisedLearning:

Unsupervised learning works without labelled data and identifies hidden patterns or unusual behaviour. It is mainly used for detecting unknown threats and zero-day attacks.

Techniquesinclude:

- K-MeansClustering
- DBSCAN
- Autoencoders

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

These methods help detect abnormal network traffic, suspicious user behaviour, and unusual system activities.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

3. Semi-SupervisedLearning:

Semi-supervisedlearning combinesboth labelled andunlabelled data.Itisusefulinsituations where collecting labelled cyber security data is difficult. This approach improves detection performance by learning from limited known threats and large amounts of available data.

4. Deep Learning:

DeeplearningtechniquesareadvancedMLmethodsthatanalyzecomplexandlarge-scaledata. They are useful for identifying sophisticated cyber threats.

Commondeeplearningmodelsinclude:

- ArtificialNeuralNetworks(ANN)
- ConvolutionalNeuralNetworks(CNN)
- RecurrentNeuralNetworks(RNN)

These models analyze network packets, system logs, and user activity sequences to detect advanced attacks.

5. ReinforcementLearning:

Reinforcementlearningallowssystemstolearnthroughinteractionwiththeirenvironment.In cybersecurity, itisusedfor automateddecision-making,such asimprovingfirewallrules and selecting appropriate responses during attacks.

6. NaturalLanguageProcessing(NLP):

NLP techniques analyze text-based information such as emails, messages, and web content. They are used for detecting phishing emails, social engineering attacks, and malicious communication patterns.

DATASETSANDDATAPREPROCESSING:

Datasets are an essential part of developing Artificial Intelligence and Machine Learning-basedcybersecuritysystems.High-qualitydatasetsarerequiredfortraining,testing, and evaluating models used for detecting threats, identifying intrusions, analyzing malware, and

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

preventing cyber fraud. Commonly used cyber security datasets include KDD Cup 99, NSL-KDD,CICIDS2017/2018,UNSW-NB15,DARPA,andBot-IoT.Thesedatasetscontain information related to network traffic, attack behaviour, system activities, and different types

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
ISSN: 2319-2992, Impact Factor 5.007
Peer-Reviewed | Open Access | International Journal
Volume: 17 | Issue: 07 | July 2026 | www.iajome.com

of cyber threats such as denial-of-service attacks, malware, unauthorized access, and probing activities.

Apart from public datasets, organizations also use real-world data sources such as firewall logs, authentication records, email communication data, and endpoint monitoring information to train security models. Data preprocessing is a critical step that improves the accuracy and efficiency of machine learning models. Raw cyber security data often contains missing values, duplicate records, noise, and inconsistent information, which must be processed before analysis.

Themainpreprocessingstepsinclude:

1. DataCleaning:

This involves removing duplicate data, correcting errors, and managing missing or incorrect values to improve data quality.

2. DataTransformation:

Raw data is converted into a suitable format for machine learning algorithms. Categorical information such as protocol types and attack labels are transformed into numerical values.

3. FeatureSelectionandExtraction:

Relevant features are selected from large datasets to reduce complexity and improve model performance. Removing unnecessary attributes helps reduce noise.

4. DataNormalizationand Scaling:

Differentfeaturesmayhavedifferentvalueranges.Normalizationensuresthatallattributesare balanced and prevents certain features from dominating the learning process.

5. HandlingImbalancedData:

In cyber security datasets, normal activities usually have more records than attack activities. Techniques such as oversampling, undersampling, and Synthetic Minority Over-sampling Technique (SMOTE) are used to balance the dataset.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

6. DataSplitting:

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

Thedatasetisdividedintotraining,validation,andtestingsectionstomeasuretheperformance and reliability of the developed model.Proper dataset selection and preprocessing are important for creating accurate, efficient, and dependable cyber security solutions.

FACTORSRESPONSIBLEFORCYBERATTACKS:

Cyber-attacks occur due to various technical, human, and organizational weaknesses. Understanding these factors helps organizations develop effective security strategies and reduce cyber risks.

1. Rapid Digitalization:

The increasing adoption of internet services, cloud computing, mobile applications, and IoT devices has expanded the attack surface. More connected systems provide attackers with additional opportunities to exploit vulnerabilities.

2. WeakSecurityInfrastructure:

Outdated software, poor security configurations, and unpatched systems create opportunities for attackers. Weak firewall policies and insufficient monitoring mechanisms increase the possibility of security breaches.

3. Human Error:

Humanmistakesareoneofthemajorcausesofcyberincidents.Usersmayunknowinglyopen phishing emails, use weak passwords, or install harmful applications. Lack of security awareness increases vulnerability.

4. PoorAuthenticationPractices:

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

Weak or reused passwords make systems vulnerable to unauthorized access. The absence of multi-factor authentication increases the risk of credential-based attacks.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

5. AdvancedAttackTechniques:

Cyber attackers continuously develop new methods using malware, ransomware, social engineering, and automated attack tools. These techniques can bypass traditional security controls.

6. InsiderThreats:

Employees, contractors, or trusted individuals with system access may accidentally or intentionally compromise security. Insider threats are difficult to detect because they involve authorized users.

7. LackofSecurityAwareness:

Organizations without proper security training, policies, and risk management practices are more likely to experience cyber incidents.

8. FinancialandPoliticalMotivation:

Many attacks are performed for financial benefits such as data theft, fraud, and ransomware payments. Some attacks are motivated by political goals, espionage, or cyber warfare.

9. PoorIncident Response:

Delayedidentificationandresponsetoattacksallowattackerstocausemoredamage.Effective monitoring and recovery plans are necessary to reduce the impact of cyber incidents.

TYPESOFTHREATAGENTS:

A threat agent refers to any individual, group, or organization capable of performing cyber attacks against digital systems and information resources. Threat agents differ based on their skills, resources, and objectives.

1. CyberCriminals:

Cyber criminals mainly perform attacks for financial benefits. They use methods such as phishing,ransomware,identitytheft,andfinancialfraudtogainillegalaccessorstealvaluable information.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

2. HackersandScriptKiddies:

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

Hackersmayattacksystemsfordifferentreasons,includingcuriosity,recognition,orpersonal goals. Script kiddies usually use existing hacking tools without advanced technical knowledgebutcanstillcreatesecurityproblems.

3. InsiderThreats:

Insiders include employees, contractors, or partners who have authorized access. They may misuse their access intentionally or accidentally expose sensitive information.

4. Nation-StateAttackers:

Nation-state groups are supported by governments and conduct highly advanced cyber operations.Theirobjectivesincludecyberespionage,politicalinfluence,andtargetingcritical infrastructure.

5. Hacktivists:

Hacktivists perform cyber attacks based on social, political, or ideological beliefs. Common activities include website attacks, information leaks, and service disruption.

LIMITATIONSOFTRADITIONALCYBERSECURITYAPPROACHES:

Traditional cyber security methods such as firewalls, antivirus software, access control systems, and signature-based detection have provided protection against many known threats. However, they face limitations when dealing with modern and rapidlychangingcyberattacks.Onemajorlimitationisthelackof adaptability. Traditional systems depend on predefined rules and require manual updates, making them less effective against new attack techniques and zero-day threats.

Another challenge is the occurrence of false positives and false negatives. Security systems may incorrectly identify normal activities as threats or fail to detect actual attacks. Traditional security solutions also struggle with scalability. The growth of cloud computing, IoT devices, and large-scale networks generates massive amounts of data that are difficult to analyzeusingconventionalmethods.Additionally,theseapproachesdependheavilyonhuman monitoring and manual investigation. Security professionals must analyze alerts and logs, whichincreasesworkloadanddelaysresponsetime.Duetotheselimitations,organizationsare

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

movingtowardAIandML-basedsecuritysystemsthatprovidefaster,adaptive,andintelligent threat detection.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

ROLEOFARTIFICIALINTELLIGENCEINCYBER SECURITY:

Artificial Intelligence (AI) has become an important technology in modern cyber security due to the increasing complexity and frequency of cyber threats.Traditional security approaches mainly depend on predefined rules and known attack patterns, which makes them less effective against new and advanced threats. AI improves cyber security by enabling systems to analyze large amounts of data, identify hidden patterns, and respond to threats automatically.

One of the major roles of AI in cyber security is threat detection and prevention. AIbased systems continuously monitor network traffic, user activities, and system behaviour toidentifysuspiciousactions.Thesesystemscandetectunauthorizedaccessattempts,malware activities, and unusual behaviour patterns before they cause serious damage.AI also plays a significant role in detecting malware and phishing attacks. By analyzing files, emails, links, and user communication patterns, AI can identify malicious content and prevent potential security risks. Natural Language Processing (NLP) techniques help detect phishing messages and social engineering attacks by examining language patterns and suspicious information. Another important application of AI is improving Intrusion Detection Systems (IDS) and IntrusionPreventionSystems(IPS).AI-basedIDSandIPSsolutionscandetectcomplexattack patterns, reduce false alerts, and improve the accuracy of security monitoring. AI supports automated incident response by performing actions such as blocking harmful activities, isolatingaffectedsystems,andgeneratingsecurityalerts.Thisreducesresponsetimeandhelps organizations minimize the impact of cyber-attacks.

Furthermore,AIhelpsinvulnerabilitymanagementbyidentifyingsecurityweaknesses andprioritizingrisksbased ontheirseverity.By continuouslylearningfrom newdata,AI-based systems provide adaptive and proactive security protection. Overall, Artificial Intelligence strengthens cyber security by improving detection speed, accuracy, automation, and decisionmaking. It works together with human expertise to create stronger and more reliable security defence mechanisms.

MACHINELEARNINGTECHNIQUESFORTHREATDETECTION:

Machine Learning techniques are widely used in cyber security to identify threats by learning patterns from large amounts of data.These techniques help systems detect abnormal behaviour, classify attacks, and predict possible security risks.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

1. SupervisedLearningTechniques:

Supervised learning models are trained using labelled datasets containing examples of both normal and malicious activities. These models classify new data based on previously learned patterns.

Commonalgorithmsinclude:

DecisionTree:

Used for classification and decision-making by creating a tree-like structure based on securityrelated features.

RandomForest:

Combinesmultipledecisiontreestoimprovedetectionaccuracyandreduceerrors.

SupportVectorMachine(SVM):

Usedtoclassifynetworkactivitiesand identifymaliciousbehaviour.

LogisticRegression:

Applied for predicting whether an activity belongs to a normal or attack category. These algorithms are commonly used in malware detection, spam filtering, and intrusion detection.

2. UnsupervisedLearningTechniques:

Unsupervised learning identifies hidden patterns without requiring labelled attack data. It is useful for detecting unknown threats and zero-day attacks.

Commonmethodsinclude:

K-MeansClustering:

Groupssimilardatapointstogether andidentifiesunusualactivities.

DBSCAN:

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

Detectsabnormalpatternsandseparatessuspiciousactivitiesfromnormalbehaviour.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

Autoencoders:

Usedtoidentifyanomaliesbylearningnormalsystembehaviouranddetecting deviations.

3. Semi-SupervisedLearning:

Semi-supervisedlearningusesacombinationoflabelledandunlabelleddata.Itimprovesthreat detection when only limited examples of cyber attacks are available. This technique is useful in large-scale networks where collecting complete labelled datasets is difficult.

4. DeepLearningTechniques:

Deeplearningmodelsanalyzecomplexandhigh-dimensionalcybersecurity data.

ArtificialNeuralNetworks (ANN):

Usedforidentifyingpatternsinsecurity-relatedinformation.

ConvolutionalNeuralNetworks(CNN):

Effectiveforanalyzingcomplexstructuressuchasnetworktrafficandmalwarefeatures.

RecurrentNeuralNetworks(RNN):

Used for analysing sequential data such as user activities and system logs. Deep learning methodsare highly effectiveindetecting advancedpersistentthreatsandsophisticated malware attacks.

5. ReinforcementLearning:

Reinforcement learningenables securitysystems to learnthrough continuous interactionwith the environment. It helps develop automatic response strategies such as improving firewall rules, blocking attacks, and selecting suitable defence actions.

6. NaturalLanguageProcessing(NLP):

NLPtechniquesareusedtoanalyzetext-basedcyberthreatssuchasphishingemails,malicious messages, and social engineering attempts. By understanding language patterns, NLP helps

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

identify suspicious communication.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

CONCLUSION:

The continuous growth of cyber threats has created the need for intelligent and adaptive securitysolutions.Traditionalcybersecuritymethodsarenolongersufficienttohandlemodern attacks due to their limited ability to detect unknown and evolving threats. Artificial IntelligenceandMachineLearningprovideadvancedapproachesforimprovingcybersecurity by enabling automated threat detection, real-time monitoring, intelligent analysis, and faster response. AI and ML techniques can identify suspicious activities, detect malware, prevent intrusions, and support effective incident management. Although challenges such as data privacy, model reliability, and adversarial attacks remain, continuous advancements are improving the effectiveness of AI-based security systems. The integration of Artificial Intelligence and Machine Learning with traditional security methods will play a major role in developing stronger, smarter, and more resilient cyber defence systems in the future.

REFERENCE:

1. **Sommer&Paxson(2010)**
   Discusses the challenges of applying machine learning to network intrusion detection systems.
2. **Buczak&Guven(2016)**
   Provides a detailed survey of machine learning and data mining techniques in cybersecurity.
3. **Patcha&Park(2007)**
   Explainsvariousanomalydetection techniquesused foridentifyingcyber-attacks.
4. **Lavalleeetal.(2009)**
   AnalyseslimitationsoftheKDDCup99datasetusedforintrusiondetection research.
5. **Shoneetal. (2018)**
   Proposesdeeplearningmodelsforaccuratenetworkintrusiondetection.
6. **Kimetal. (2014)**
   Introducesahybridintrusiondetectionapproachcombiningmisuseandanomaly detection.
7. **Lippmannetal.(2000)**
   EvaluatesintrusiondetectionsystemsusingtheDARPAdataset.
8. **Moustafa&Slay (2015)**
   PresentstheUNSW-NB15datasetformodernintrusiondetectionexperiments.
9. **Sharfuddinetal.(2018)**
   IntroducesCICIDS2017datasetreflectingreal-worldnetwork attacks.
10. **Goodfellowetal.(2014)**
    Explainsadversarialattacksthatcanfoolmachine learning models.
11. **Scikit-learn**
    Provideswidelyusedmachine learningalgorithmsforcybersecurityresearch.
12. **TensorFlow**

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

Supportsdeeplearningmodelsforthreatdetectionandanalysis.

13. **MITREATT&CK**

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

Offersaknowledgebaseofadversarytacticsandtechniques.

14. **Cisco Security**
    AppliesAItodetectandrespondtoenterprisecyberthreats.
15. **IBMSecurity**
    Usesmachinelearningforadvancedthreatintelligenceand analytics.
16. **Symantec**
    EmploysAI-basedsystemsformalwareandendpointprotection.
17. **FireEye**
    FocusesondetectingadvancedpersistentthreatsusingAI.
18. **ENISA**
    PublishesreportsonAIapplicationsinEuropeancyber security.
19. **NIST**

    ProvidesstandardsandguidelinesforsecureAI systems.

20. **IEEEXplore**

    AdigitallibraryforresearchonAIandMLincybersecurity.