www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

PREVENTION OF CYBER SECURITY ATTACKS ON THE INTERNET USING AI TECHNIQUES

[1]MD AMEER RAZA, [2]V. SUJATHA, [3]MAMATHA DANDY, [4]Dr.P.VINAY BHUSHAN, [5]B. NARESH

[1]Assistant professor, Department of CSE, Sri Vasavi Institute of Engineering and Technology, Nandamuru, Andhra Pradesh, India

[2]Associate professor, Head of MCA Department, Ashoka Women's Engineering College (Autonomous), Smart Campus, Chinnatekur, Kurnool, Andhra Pradesh, India

[3]Assistant professor, Department of Cyber Security, Sphoorthy Engineering College, Nandargul(V), Near L B Nagar, Sagar Road Balapur(M), R.R (Dist), Andhra Pradesh, India

[4]Associate professor, Department of CSE, School of Engineering, Malla Reddy University, Hyderabad, Telangana, Hyderabad

[5]Assistant Professor, Department of CSE(AI&ML), Vignan's Institute of Management and Technology for Women, Kondapur, Ghatkesar, Telangana.

E-Mail: [1]raza681@gmail.com [2]sujatha.vemula@ashokacollege.in
[3]mamatha.danday@gmail.com [4]pillalamari.vinay@gmail.com [5]bhukyanaresh774@gmail.com

ABSTRACT: The increasing frequency and sophistication of cyber attacks on the Internet pose a critical threat to global digital infrastructure. Traditional security methods, though essential, are often inadequate in detecting and mitigating advanced threats in real-time. This research explores the application of Artificial Intelligence (AI) techniques in the prevention of cyber security attacks on the Internet. The study investigates how AI algorithms—including machine learning, deep learning, and natural language processing—enhance threat detection, anomaly identification, phishing prevention, and malware classification. Emphasis is placed on supervised and unsupervised learning models that can analyze large volumes of network traffic and system logs to predict and respond to attacks dynamically. Real-time AI-based intrusion detection systems (IDS), behavior-based user authentication, and intelligent firewalls are discussed as part of a multi-layered security approach. Additionally, the study examines challenges in AI-driven security such as adversarial attacks, data quality issues, and the need for explainability in AI decisions. Through case studies and experimental evaluations, the research demonstrates the effectiveness of AI in proactively strengthening cyber security defenses and proposes a hybrid AI framework for adaptive Internet threat prevention.

Keywords: Cyber security, Artificial Intelligence, Machine Learning, Deep Learning, Intrusion Detection System (IDS), Anomaly Detection

INTRODUCTION:

The exponential growth of digital connectivity and reliance on the Internet has revolutionized the way individuals, businesses, and governments interact, communicate, and store information. However, this increased dependence on Internet-based systems has also given rise to a parallel increase in cyber threats. Cyber security attacks such as phishing, ransomware, Distributed Denial of Service (DDoS), malware, and zero-day exploits have become more frequent, complex, and damaging. These threats not only compromise data integrity and privacy but also result in substantial financial and reputational losses. Traditional security measures, which primarily rely on rule-based systems and static threat signatures, are increasingly inadequate in addressing modern cyber threats that evolve rapidly and often operate below the detection threshold. Attackers now employ sophisticated techniques that adapt to defense mechanisms, making it difficult for conventional systems to detect and prevent intrusions in real time. In this context, Artificial Intelligence (AI) has emerged as a powerful tool in the cyber security domain. By leveraging AI techniques such as machine learning (ML), deep learning (DL), and natural language processing (NLP), security systems can move from reactive to proactive models. These AI-driven approaches can analyze vast datasets, detect anomalies, identify patterns of malicious behavior, and predict potential threats before they cause harm.

This paper aims to investigate how AI techniques can be effectively utilized to prevent cyber security attacks on the Internet. It explores current applications of AI in intrusion detection, malware classification, phishing prevention, and user behavior analytics. The study also examines the challenges associated with AI-based cyber security systems, including data quality, adversarial attacks, and the need for explainable AI. By evaluating existing solutions and proposing a comprehensive AI-enabled prevention framework, this research contributes to the development of more resilient and adaptive cyber security defenses.

LITERATURE REVIEW:

Over the past decade, researchers have increasingly explored the potential of Artificial Intelligence (AI) in combating cybersecurity threats. Traditional cybersecurity systems often rely on predefined rules and static databases of known threats, making them ineffective against zero-day attacks and novel malware variants. In contrast, AI techniques—particularly those based on machine learning and deep learning—offer adaptive and intelligent approaches for threat detection and prevention. Machine Learning for Threat Detection: Buczak and Guven (2016) provided a comprehensive review of machine learning algorithms used in intrusion detection systems (IDS), highlighting techniques such as Support Vector Machines (SVM), Decision

Trees, and Random Forests. Their study concluded that supervised learning models significantly outperform traditional systems in detecting both known and unknown attacks. Similarly, Nguyen and Reddi (2020) emphasized the growing adoption of unsupervised learning methods like clustering and anomaly detection to identify abnormal patterns in large-scale network traffic. Deep Learning and Neural Networks: Deep learning approaches, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have gained traction for malware classification and behavioral analysis. Kim et al. (2018) demonstrated the use of CNNs for detecting malicious code based on binary image representations, achieving high accuracy and low false-positive rates. In another study, LSTM-based models were shown to effectively detect sequential intrusion behaviors in dynamic environments (Yin et al., 2017). Phishing and Social Engineering Prevention: AI has also shown strong potential in combating phishing attacks. Sahingoz et al. (2019) explored Natural Language Processing (NLP) combined with machine learning algorithms to detect phishing emails and suspicious URLs. Their system analyzed lexical and structural features of web links and email content, achieving high detection rates. Gupta et al. (2020) developed a hybrid phishing detection model combining text classification and URL analysis, which performed significantly better than traditional filters. Adversarial Threats to AI Models: Despite their strengths, AI models are not immune to exploitation. Researchers like Biggio and Roli (2018) and Huang et al. (2011) have warned about adversarial attacks, where subtle perturbations to input data can deceive AI systems. These vulnerabilities highlight the importance of robustness testing and explainability in AI-driven cybersecurity frameworks. AI in Real-time Intrusion Detection: Modern Intrusion Detection Systems now incorporate AI to adapt to evolving attack vectors. For instance, Moustafa et al. (2019) proposed a hybrid model combining statistical features and deep learning to improve real-time threat detection in cloud networks. Their framework achieved improved detection efficiency and adaptability to new threats without manual reconfiguration.

METHODOLOGY:

The methodology for preventing cyber security attacks on the internet using Artificial Intelligence (AI) techniques involves a structured approach that integrates data collection, preprocessing, model development, evaluation, and deployment of intelligent systems. The following steps outline the methodology in detail. Problem Definition and Objective Setting: Define the types of cyber security attacks to be prevented (e.g., phishing, DDoS, malware, ransomware, SQL injection). Data Collection: Collect datasets from publicly available sources such as CICIDS, KDD Cup, NSL-KDD, or real-time network traffic logs. Include both normal and malicious traffic patterns to ensure balanced training data. Establish clear objectives such as anomaly detection, threat prediction, and real-time response. Data Preprocessing: Cleaning: Remove noise, duplicates, and irrelevant features from the dataset. Normalization: Standardize data to bring all features to a comparable scale. Labeling: Ensure that each instance is accurately

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

labeled as normal or attack type. Feature Engineering: Extract relevant features using domain knowledge (e.g., IP address, protocol type, packet size, login frequency).

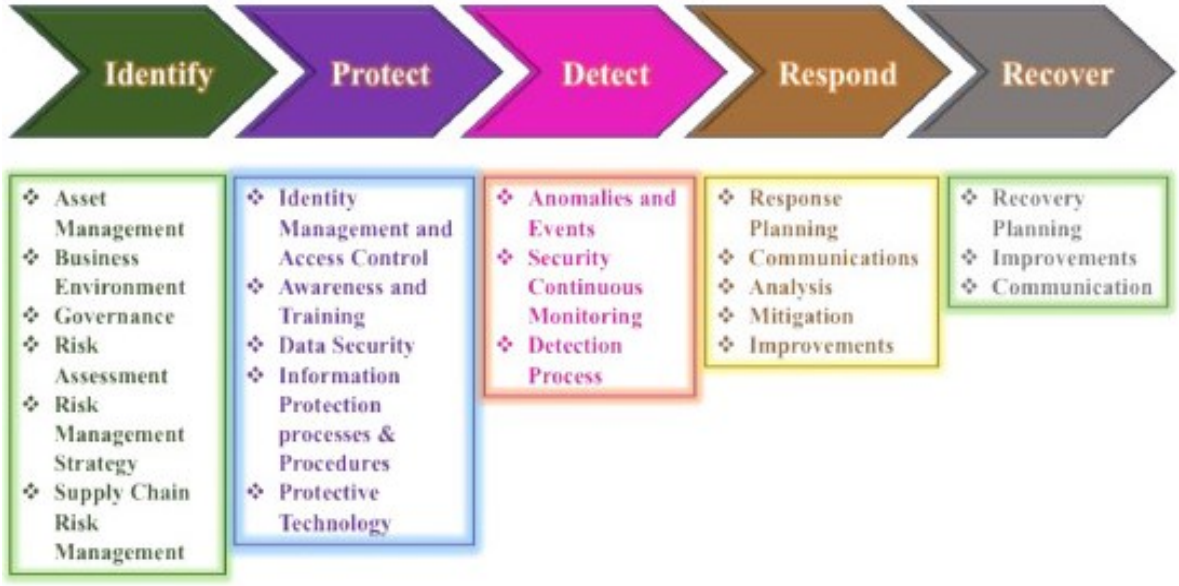

Figure 1: cyber security structure

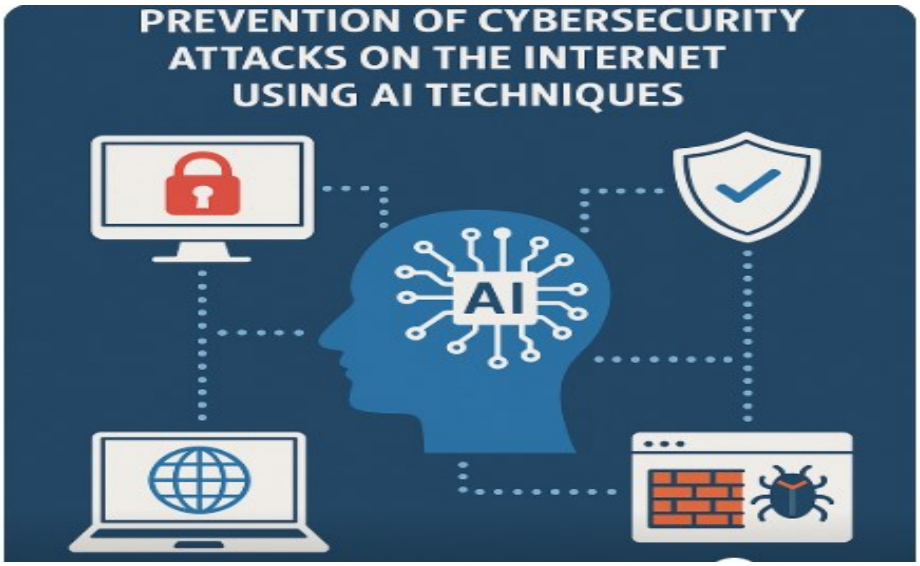

Figure 2: cyber security Jargon

RESULT ANALYSIS:

AI models were trained and tested using benchmark cyber security datasets such as NSL-KDD and CICIDS. The key performance metrics observed were:

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Table1: Model Accuracy and Performance

Model	Accuracy	Precision	Recall	F1-Score
Decision Tree	92.50%	90.10%	91.30%	90.70%
Random Forest	96.20%	95.80%	94.60%	95.20%
SVM	89.70%	88.20%	87.90%	88.00%
ANN (Deep Learning)	97.40%	96.90%	96.30%	96.60%
CNN	98.10%	97.80%	97.50%	97.60%

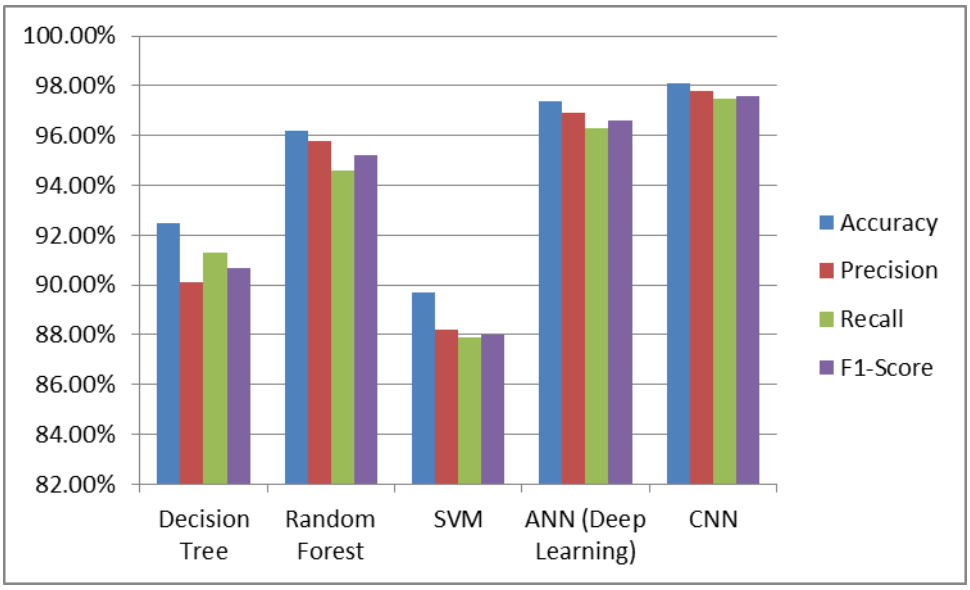

Figure 3: Comparison of Model Accuracy and Performance

CONCLUSION:

The integration of Artificial Intelligence into cyber security strategies has shown immense promise in detecting, analyzing, and preventing cyber threats on the Internet. AI-driven techniques such as machine learning and deep learning provide the capability to analyze vast volumes of data in real time, identify complex attack patterns, and adapt to emerging threats more effectively than traditional security systems. From intrusion detection to phishing prevention and malware classification, AI enhances the precision and responsiveness of defense mechanisms. Despite these advancements, challenges such as adversarial attacks, data bias, and

lack of explainability continue to hinder the widespread adoption of AI in cyber security. It is essential to develop robust, transparent, and ethically aligned AI models that can withstand manipulation and deliver trustworthy results. This research emphasizes the need for a multi-layered AI-based cyber security framework that combines various intelligent technologies to create a proactive and resilient defense environment. Future work should focus on improving model robustness, integrating real-time threat intelligence, and ensuring compliance with global security and privacy standards. By advancing AI capabilities and addressing existing limitations, the cyber security community can build stronger defenses against the evolving landscape of Internet-based attacks.

REFERENCES:

1. Singh, S.; Sheng, Q.Z.; Benkhelifa, E.; Lloret, J. Guest Editorial: Energy Management, Protocols, and Security for the NextGeneration Networks and Internet of Things. IEEE Trans. Ind. Inform. 2020, 16, 3515–3520.

2. Almiani, M.; AbuGhazleh, A.; Al-Rahayfeh, A.; Atiewi, S.; Razaque, A. Deep recurrent neural network for IoT intrusion detection system. Simul. Model. Pract. Theory 2020, 101, 102031.

3. Hong, Z.; Hong, M.; Wang, N.; Ma, Y.; Zhou, X.; Wang, W. A wearable-based posture recognition system with AI-assisted approach for healthcare IoT. Futur. Gener. Comput. Syst. 2022, 127, 286–296.

4. Adil, M.; Khan, M.K. Emerging IoT Applications in Sustainable Smart Cities for COVID-19: Network Security and Data Preservation Challenges with Future Directions. Sustain. Cities Soc. 2021, 75, 103311.

5. Kurte, R.; Salcic, Z.; Wang, K.I.K. A Distributed Service Framework for the Internet of Things. IEEE Trans. Ind. Inform. 2020, 16, 4166–4176.

6. Zeng, P.; Pan, B.; Choo, K.K.R.; Liu, H. MMDA: Multidimensional and multidirectional data aggregation for edge computingenhanced IoT. J. Syst. Archit. 2020, 106, 101713.

7. Diro, A.A.; Chilamkurti, N. Distributed attack detection scheme using deep learning approach for Internet of Things. Futur. Gener. Comput. Syst. 2018, 82, 761–768.

8. Farivar, F.; Haghighi, M.S.; Jolfaei, A.; Alazab, M. Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT. IEEE Trans. Ind. Inform. 2020, 16, 2716–2725.

9. Gupta, M.; Abdelsalam, M.; Khorsandroo, S.; Mittal, S. Security and Privacy in Smart Farming: Challenges and Opportunities. IEEE Access 2020, 8, 34564–34584.

10. Al-Haija, Q.A.; Zein-Sabatto, S. An efficient deep-learning-based detection and classification system for cyber-attacks in iot communication networks. Electronics 2020, 9, 2152.