A Comprehensive Review on Operational Uses, Risk and Future Trends of AI Cyber Defensive Mechanisms against Advanced AI-Generated Malicious Threats

Submitted By

MD. Mohinuzzaman Tushar

ID: 202-35-652

Department of Software Engineering

Daffodil International University

Supervised By

Dr. A. H. M. Saifullah Sadi

Professor

Department of Software Engineering

Daffodil International University

Bachelor of Science in Software Engineering

DAFFODIL INTERNATIONAL UNIVERSITY

APPROVAL

This thesis is titled"**A Comprehensive Review on Operational Uses, Risk and Future Trends of AI Cyber Defensive Mechanisms against Advanced AI-Generated Malicious Threats**", submitted by **Md. Mohiuzzaman Tushar (ID: 202-35-652)** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

Fazla Elahe

Chairman

Dr. Md. Fazla Elahe
Assistant Professor & Associate Head
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Marzia

Internal Examiner 1

Dr. Marzia Ahmed
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

13.09.2025

Internal Examiner 2

Dr. Shabnam Mustary
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

13.09.25

External Examiner

Mohammod Abul Kashem
Professor
Department of Computer Science and Engineering
Dhaka University of Engineering & Technology, Gazipur.

DECLARATION

I want to state that this thesis was carried out under the supervision of Dr A. H. M. Saifullah Sadi, Professor in the Department of Software Engineering at Daffodil International University.I hereby declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the Bachelor of Science in Software Engineering Major in Cyber security at Daffodil International University. I also confirm that this work in whole or in part has not been submitted for any other academic qualification.

Submitted by :

Tushar

Md. Mohiuzzaman Tushar
ID : 202-35-652
Department of Software Engineering
Daffodil International University

Certified by :

15/9/2025

Dr. A. H. M. Saifullah Sadi
Professor
Faculty of Science and Information technology
Department of Software Engineering
Daffodil International University

ACKNOWLEDGEMENT

Firstly, it is my utmost pleasure to dedicate this work to my dear parents and my family, who granted me the gift of their unwavering belief in my ability to accomplish this goal: thank you for your support and patience. I wish to express my appreciation and thanks to those who provided their time, effort and support for this thesis. To the members of my dissertation committee, thank you for sticking with me. Finally, a special thanks to Prof. Dr. A.H.M. Saifullah Sadi for his continuous support, encouragement, and leadership, and for that, I will be forever grateful.

DEDICATION

I dedicate this work to my mentors and instructors; thank you for mentoring me with your wisdom and expertise; this has been much helped in crafting my work. Finally, I dedicate my thesis to all future academics and students aiming to significantly contribute in the subject of fog computing security and cybersecurity. This work should motivate more creativity and commitment in striving greatness.

ABSTRACT

The use of Artificial intelligence in Cyber defensive Security is growing day by day. At the same time, the Cyber terrorism unit(CTU) is growing more advanced by the use of AI generated malicious tools and techniques. The rapid advancement of Artificial intelligence has led to emergence of AI generated malicious threats including polymorphic malware, adversarial attacks, AI social engineering and AI ransomware etc. To counter this risk, organizations are increasingly adopting the use of AI-Power defensive mechanisms. Generative AI(GAI) can provide organizations an additional layer of defence against increasing AI generated sophisticated attacks. In this article, we have discussed the challenge of using AI integrated defensive security against the more advanced hackers or malicious actors. The study organizes AI - Related threats into two main categories: the first AI components such as algorithms, frameworks and data the second one is malicious activity of AI such as large scale cyber attacks .By analyzing these challenges , the work support a threat-informed defense strategy through risk assessment approaches tailored for AI security.

Keywords-AI-generated attacks, Adversarial attacks, AI defensive security, Risk assesments, Predictive analytics.

Table of Contents

List of Figures

List of Tables

CHAPTER 1

INTRODUCTION

In today's landscape, cybersecurity stands as a critical concern for individuals, organizations and governments around the world. Cybercriminals are utilizing increasingly complex methods to exploit digital systems. Cyberthreats have grown increasingly sophisticated and frequent. Successful cyberattack can lead to severe consequences such as financial losses, data breaches, and damage to reputation .The nature of cyber threats has become increasingly sophisticated and intricate.In this context robust security measures have become critically important. It is more important than ever to have strong cybersecurity safeguards in place (Nagar, 2024) AI technology acquires and adjusts to new threats and methods of attacks, allowing defense systems to advance alongside emerging cyber risk. Utilizing adaptive learning and recognizing patterns,AI-driven solutions can proactively detect and mitigate threats as they occur, staying one step ahead of cyber attackers.(Dwivedi, 2025)

1.1 Background information

It is more important than ever to have strong cybersecurity safeguards in place. AI technology acquires and adjusts to new threats and methods of attacks, allowing defense systems to advance alongside emerging cyber risk. Utilizing adaptive learning and recognizing patterns,AI-driven solutions can proactively detect and mitigate threats as they occur, staying one step ahead of cyber attackers.(Altun, 2024)

Sophisticated AI-generated attack

Automated reconnaissance and targeting

AI (such as generative AI and predictive analytics) is used in defensive security's automated reconnaissance and targeting to proactively scan networks, find weaknesses, and rank threats. By contextualizing threats and automatically mapping attack surfaces, it speeds up threat hunting and response. Operational risks are introduced, though, such as the disclosure of vital assets, disruptive activities brought on by false positives, or the use of assaults by adversaries to hone in on specific targets. Adversarial testing and strict oversight are necessary for safe deployment.

AI-generated social engineering and phishing attacks

Generative AI is used in AI-generated social engineering and phishing attempts to produce highly tailored and convincing lures (voice clones, emails, and messages) on a large scale. (Rangrez, 2024).They circumvent conventional filters, imitate reliable sources, and take advantage of human psychology by using familiarity or urgency. This significantly raises the success rates of malware deployment, penetration, and credential theft. AI-enhanced linguistic anomaly detection, behavioral analysis, and ongoing user education on changing strategies are all necessary for defending.(Zomaya, 2023)

AI Evolve Malware

AI-evolved malware automatically changes its code, behavior, and attack vectors in real-time by utilizing machine learning (e.g., GANs, reinforcement learning). It detects zero-day exploits, evades signature-based protections, and adjusts to avoid heuristic analysis. Threats become "living" as a result, continuously learning from defensive reactions(Zhang, 2023). Predictive threat hunting to foresee new varieties, adversarial training, and AI-driven detection (such as behavioral analytics) are necessary to combat it

Automated attack infrastracture

AI is used by automated attack architecture to plan malicious domains, compromised servers, and self-managing botnets(Nagar, 2024). It scales attacks globally, rotates TTPs (Tactics, Techniques, Procedures), deploys payloads (such AI malware), and automatically looks for weaknesses. This enables relentless, adaptive assaults (DDoS, ransomware) with minimal human input. Defenders require AI-driven threat intelligence and automated containment to disrupt command-and-control (C2) networks and mitigate swarm-like offensive operations[Sing and Dubey, 2024]

AI-enhanced disinformation

AI-enhanced disinformation leverages generative models (LLMs, GANs) to mass-produce hyper-realistic fake content — deepfake videos, forged documents, and social media bot swarms tailored to exploit cultural/emotional triggers[Aitan, 2024]. At a speed and scale never seen before, it deepens divisiveness, sways public opinion, and undermines institutional trust. Media literacy initiatives, blockchain-verified provenance, AI-driven synthetic media detection, and coordinated platform responses to false narratives that spread online are all necessary to combat it.(Zomaya, 2023)

Intelligence attack automation

AI is used in intelligence attack automation to collect, evaluate, and weaponize target data (such as network configurations, employee profiles, and vulnerabilities) on its own. In order to prioritize valuable assets, create customized exploits, and carry out precision strikes without human assistance, it connects data from many sources(Zhang, 2025). This enables hyper-efficient, continuous offensive campaigns. Countermeasures demand AI-enhanced threat intelligence, automated deception systems, and proactive hunting to disrupt reconnaissance loops pre-emptively(Kumari, 2025).

AI in cyber defensive mechanisms

AI/ML algorithms are used in anomaly detection to create behavioral baselines (network, user, and system) and instantly identify and highlight notable deviations. In order to differentiate between false positives and actual attacks (such as intrusions or data exfiltration), attack identification examines these anomalies and correlates them with threat intelligence. While critical for spotting novel threats, it faces challenges like adversarial evasion and alert fatigue, requiring human expertise for validation and response prioritization(Saurabh, 2024).

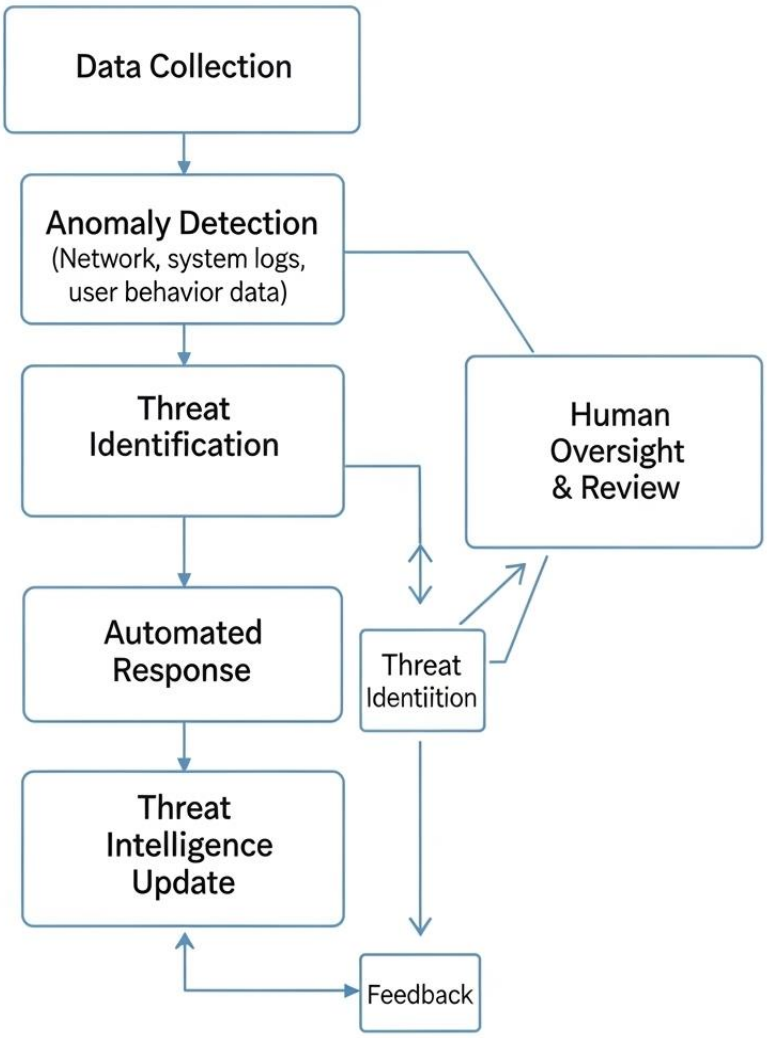


Figure 1.1: AI Cyber Defensive Mechanism

AI/ML models are used in automated threat detection and prediction to examine threat intelligence and real-time data (such as network traffic and logs). By identifying attacker TTPs (Tactics, Techniques, Procedures) and analyzing trends, it predicts future threats and detects active attacks through anomaly detection. Proactive defense preemptively fixing vulnerabilities or thwarting new campaigns is made possible by this. Challenges include reducing false predictions and ensuring models adapt to novel attack vectors without human oversight delays(Kumari, 2024).

AI/ML is used in automated incident detection to continually scan logs, networks, and systems for aberrant activity or indicators of compromise (IoCs). It detects patterns (such as lateral movement and data exfiltration), correlates alerts in real-time, and initiates alerts automatically. This accelerates response but risks false positives and alert fatigue. Integration with SOAR platforms enables automated containment while

human oversight ensures critical context and validation.Through layered controls, phishing and social engineering security counteracts(Saddi, 2024).AI-hyperpersonalized attacks (deepfakes, bogus emails):Technical: DMARC/SPF authentication, URL sandboxing, and AI email filters.Reporting procedures, ongoing training (attack simulation). Using behavioral analytics to identify unusual data access or logins.Zero Trust: Strict access controls limiting breach impact.Success hinges on integrating AI tools with human vigilance and iterative policy updates against evolving lures(Rangrez, 2024).

AI-generated vulnerability Management

AI-generated vulnerability management uses machine learning to automate the processes of finding, evaluating, and prioritizing vulnerabilities. By examining code, configurations, and threat intelligence, it simulates attack routes and forecasts exploitable vulnerabilities. AI prioritizes risks based on exploit likelihood and impact, accelerating patching. It also generates remediation scripts(Zomaya, 2023). Challenges include false positives and adversarial poisoning of training data, requiring human validation and robust model governance to maintain trust in automated outputs(Sing and Dubay, 2024).Deception technology proactively deploys realistic decoys (fake systems, data, credentials) across networks to mislead attackers. Alerts are immediately triggered when adversaries engage with these traps, disclosing their location, strategies, and goals without affecting actual assets. AI enhances decoy realism and adapts lures based on attacker behavior(Nagar, 2024). This provides early detection, reduces false positives, and gathers actionable threat intelligence—critical for disrupting automated or AI-driven attacks early in the kill chain(Dwived, 2025).

1.2 Motivation of the Research

An important turning point in cybersecurity is the quick development of artificial intelligence (AI), especially generative AI (GAI). Advanced malicious actors and cyber terrorism units (CTUs) are among the smart enemies who are using this technology as a weapon, despite the fact that it offers previously unheard-of capabilities for strengthening protective measures. The primary driving force behind this research is the urgent and asymmetric danger picture created by this convergence. Malicious actors are using AI more and more to create increasingly complex, evasive, and scalable threats. These include adversarial attacks that try to trick AI-driven detection systems, hyper-personalized AI social engineering campaigns, automated AI ransomware operations, and polymorphic malware that changes to evade signatures.

Traditional, human-centric defensive strategies are outpaced by the machine-speed evolution of these threats(Faruqi and Siam, 2025).

1.3 Problem Statement

Today's threat landscape results from the growing sophistication of AI-generated hostile threats (such as polymorphic malware, adversarial attacks, and AI ransomware) surpassing traditional cyber defenses. In order to combat these changing threats, businesses are increasingly implementing AI-powered defensive mechanisms, such as Generative AI (GAI). However, the operational integration of defensive AI has inherent vulnerabilities. These weaknesses result from the possibility of offensive AI undermining defensive systems or facilitating extensive attacks, as well as exploitable AI components (algorithms, data, and frameworks). Importantly, the operational risks associated with utilizing AI defensively against attackers equipped with AI are not sufficiently addressed by current cybersecurity frameworks.

1.4 Research Questions

Question 01 : What are the distinguishing traits and patterns of development of dangerous threats created by AI (such as polymorphic malware, adversarial attacks, AI social engineering, and AI ransomware) in the context of offensive use by sophisticated actors (such as CTUs)?

Question 02: What are the main operational applications, capacities, and constraints of both established and new AI-powered defenses (such as predictive analytics and generative AI, or GAI) in thwarting complex AI-generated threats

Question 03 : How can the resilience and efficacy of AI-powered cyber defenses against changing AI-generated threats be improved by the development and implementation of a threat-informed defense strategy that includes customized risk assessments and mitigations for AI-specific vulnerabilities?

1.5 Research Objectives

Organize and describe changing hostile threats created by AI in a methodical manner, paying particular attention to how they exploit AI flaws and how they affect operations.

i.To develop specialized approaches for evaluating the distinct operational risks—such as algorithmic flaws, data contamination, and systemic failures

ii.To introduce it by using defensive AI against adversaries equipped with AI.

iii.To create practical recommendations and mitigation techniques for putting in place risk-aware, flexible, and resilient AI-powered cyber defenses against sophisticated AI-generated threats.

1.6 Research Scope

Organize and describe changing hostile threats created by AI in a methodical manner, paying particular attention to how they exploit AI flaws and how they affect operations. Examples of these threats include adversarial attacks, polymorphic AI malware, and AI-driven social engineering.

i.Examine critically the practical applications, efficacy, and intrinsic drawbacks of both established and new AI-driven defenses (such as generative AI and predictive analytics) against complex AI-generated threats.

ii.Develop specialized approaches for evaluating the distinct operational risks—such as algorithmic flaws, data contamination, and systemic failures—introduced by using defensive AI against adversaries equipped with AI.

CHAPTER 2

Literature Review

2.1 Introduction

The rapid evolution of cybersecurity has catalyzed a dual edge transformation in cyber security. While AI enhances defensive capabilities through advanced threat detection and automated response, it simultaneously empower cyber adversaries to develop sophisticated AI generated threats, including polymorphic malware, adversarial attack, AI driven social engineering and autonomous ransomware.Utilizing Generative AI for Threat Simulation: Generative adversarial networks (GANs) and variational autoencoders (VAEs) are employed to produce realistic attack scenarios (such as polymorphic malware and phishing emails) that help in evaluating defense mechanisms. Organizations leverage these simulations to enhance intrusion detection systems (IDS) and improve response strategies, yielding a 15–20% increase in detection accuracy compared to signature-based approaches (Vadisetty & Polamarasetti, 2024).

Table 2.1: Finding of the previous work on AI Generated Attack and AI defensive Mechanism

Title	Authors	AI techniques and Methods used	Contribution	Limitation
Artificial Intelligence in Cyber Defense: A study of Modern Security	Shweta Dwivedi, Naushad Varish, and Priyanka	Decision Tree,SVM,RNN,CNN	The research investigates the ways in which artificial intelligence	The document emphasizes the constraints associated with adversarial attacks on

Solutions			improves threat detection, incident response, and intrusion detection systems within the realm of cybersecurity, showcasing notable advancements in both accuracy and response times. Additionally, it addresses challeng	artificial intelligence systems and the difficulties in achieving model explainability, which may impede trust and efficacy.Furthermore, issues regarding scalability and data privacy present considerable obstacles to the extensive deployment of AI in the field of cybersecurity.

			es including adversarial attacks, data privacy concerns, and the necessity for continuous innovation to maintain strong protection.	
Revolutionizing Malware Detection technique by using Predictive AI	Anurag Singh, Kanishka, and Sanjay Kumar Dubey	Random Forest,KNN,,XGBoost,AI Powered Threat Intelligence	This paper makes a significant contribution by creating AI-driven threat intellige	The limitations of the paper encompass a concentration on particular machine learning algorithms,

			nce systems that utilize Random Forest, KNN, and XGBoost algorithms to enhance the detection and mitigation of cyber threats. It highlights the importance of empirical evaluation in optimizing these models	neglecting to consider their scalability or effectiveness when applied to large and varied datasets.Furthermore, it fails to investigate the challenges associated with real-time deployment or the incorporation of these models into current cybersecurity frameworks.

			for a more effective cybersecurity defense.	
Empowering Cyber Defence by Unveiling AI powered expert System and Software Engineering	Lo'ai Tawalbeh, John Franklin, Christian Ramirez, Jonathan Garcia, Abdelrahman Tawalbeh, and Fadi Muheidat.	NLP,Deep learning,Intrusion detection trees	The document seeks to elucidate the software engineering principles that underpin artificial intelligence (AI) and its role in facilitating expert machines utilized in cyber defense	The main limitation of the paper lies in the significant dependence of expert systems on the precision of their knowledge base and training data, since erroneous information can result in detrimental decisions. Furthermore, certain detection techniques,

			systems. It examines the complex functionalities of AI within the realm of cybersecurity, encompassing deep learning, intrusion detection trees, natural language processing, and artificial immune systems. Additionally, the document offers a	such as signature-based intrusion detection systems, are constrained by their incapacity to identify novel or unregistered malicious patterns.

			summary of software engineering methodologies for AI-driven systems, highlighting their implementation in cybersecurity penetration.	
Cyber Attack Defense System Enhanced by Artificial Intelligence	Usman, Syed, Ashok,jothi	Gradient Boosting and Ensemble Learning for efficient detection of cyber threats.	This paper makes a significant contribution to the domain of cybersec	The limitations of the paper encompass inconsistent accuracy in identifying particular types of attacks, resulting in

			urity by creating an advanced Intrusion Detection System (IDS) that utilizes machine learning to improve the accuracy and adaptability of threat detection across different network architectures. Additionally, it offers importa	increased false positive rates, as well as dependence on the NSL-KDD dataset, which could influence its applicability in real-world scenarios. Additionally, it emphasizes the need for further research to improve detection capabilities for specific attacks.

			nt insights into the development, methodologies, and future directions of AI-Powered Cyber Security Defender Systems.	
Artificial Intelligence in Cybersecurity: Enhancing Automated Defense Systems to Fight Advance	Prakash,Murugasen,Poongothi, Shivakumar,vijaykumar	ML,DL,NLP,Predictive analytics,Anomaly detection	The document emphasizes that the integration of AI in cybersecurity encounters	This study explores the incorporation of artificial intelligence in cybersecurity to improve automated defense strategies against advanced

d Cyber Threats and Ensure Digital Resilience			obstacles such as the necessity for high-quality data and susceptibility to adversarial attacks. Ethical issues, including data privacy and algorithmic bias, as well as the risk of AI systems creating new vulnerabilities if not adequately	cyber threats. It evaluates the efficiency of AI-augmented systems regarding precision, rapidity, and flexibility, showcasing their enhanced performance compared to conventional approaches.

			secured, are also acknowledged. Additionally, the significance of explainability and transparency in AI decision-making is highlighted as a present limitation.	
A Review of use of Artificial Intelligence of Cyber Security	Dangi,Kumud,Nilanjon,Vaseem,Balakrisna	ML,Supervised, Unsupervised, IDS	A major contribution is the examination of pertinent	The document recognizes that cybersecurity systems powered by AI

and Fifth Generation Cyber attacks and its analysis			literature regarding the benefits of AI in the field of cybersecurity. This encompasses an evaluation of the abilities of AI-driven systems to detect malware attacks, offer effective protection against phishing and spam emails, as well	necessitate considerable data and processing capabilities. A primary constraint is the likelihood of recurrent false alarms, which may diminish efficiency. Additionally, AI systems are susceptible to threats such as malicious inputs or data corruptions.

			as safeguard networks from intrusions and prevent data breaches.	
On the choice of Effective Artificial Methods for Cyber Defence of Industrial System	Trifonov,Monalov,Tsochev	Self-learning, Reinforcement,Predictive Analysis	The Contribution for choosing Artificial Intelligence (AI) techniques for cyber defense within Industrial Automation and Control Systems (IACS),	The conclusions of the paper are mainly advisory in nature, lacking definitive categorical evidence. The methods employed for risk identification, although effective in the context of railroad

			with a particular emphasis on Functional Safety.	transport, may prove more challenging to implement in other industrial domains.
Unveiling the Next Generation of Cyber Security: Exploring AI Powered Defence Mechanisms	Gourov,Nagar	Dynamic Modeling,Threat Intelligence	This document examines the incorporation of Artificial Intelligence (AI) within the realm of cybersecurity, emphasizing its transformative capabilities.It	The document suggests approaches to tackle the ethical considerations and constraints, including the establishment of strong data privacy protocols, the reduction of algorithmic biases via routine evaluations,

			elaborates on AI's role in improving threat detection, facilitating proactive prevention, streamlining incident response, and developing adaptive defense strategies against the ever-changing landscape of cyber threats.T	the improvement of transparency and clarity in AI decision-making, the promotion of collaboration between humans and AI, the creation of solid protections against adversarial threats, and the commitment to ongoing enhancement through research and development.

			he study also considers significant ethical issues related to AI in security, including privacy challenges and algorithmic bias.	
Applications of Artificial Intelligence in Network Security and Network Defence	XIUPING CHAN	Artificial Neural Networks,Fuzzy Logic, Intelligence filter technology,	The document illustrates that artificial intelligence methods, such as neural networks and	The document primarily concentrates on AI-augmented firewalls, lacking comprehensive details on real-world implementa

			fuzzy logic, greatly enhance network security compared to conventional approaches. It suggests the implementation of AI-augmented firewalls, spam detection mechanisms, and intrusion detection systems to achieve	tions. It examines a restricted range of AI methodologies, omitting more recent approaches such as deep learning. The experiments are limited to specific types of attacks, failing to encompass all potential network threats. Furthermore, it does not consider the scalability of AI or the adaptation to evolving threats.

			more precise and adaptable protection. Experimental findings indicate a 15% increase in interception rates with AI-driven firewalls. The document emphasizes the capability of AI in managing nonlinear and fuzzy	

			data within intricate network settings. In summary, it lays the groundwork for intelligent and cooperative network defense systems.	

Artificial Intelligence Based Cyber Security threats identification in Financial Institution Using Machine Learning Approach	Drive,probhajan	SVM,NLP,Predictive analytics,Anomaly Detection	The document presents a framework based on machine learning to identify cyber threats in financial institutions in real-time, utilizing anomaly detection and Support Vector Machines (SVM). It incorporates	The limitations of the paper encompass a dependence on conventional machine learning models such as SVM, which might find it difficult to cope with the emergence of advanced threats when compared to deep learning techniques. Additionally, it does not provide an in-depth examination of the

			Natural Language Processing (NLP) to enhance phishing detection. The model shows favorable comparisons with existing methods, indicating competitive performance.	challenges related to real-time scalability within extensive financial networks.

AI models examine network traffic patterns to detect anomalies that may suggest zero-day exploits or advanced persistent threats (APTs). Deep learning models (like CNNs and RNNs) attain detection rates of 95% for APTs, in contrast to 70% for conventional systems.AI collaborates with Security Information and Event Management (SIEM) systems to streamline threat containment processes. AI

shortens incident response durations from hours to less than 15 minutes by autonomously blocking malicious IP addresses or deploying patches (Rangrez et al., 2024).Machine learning algorithms predict potential attack paths by examining threat intelligence gathered from dark web discussions and past breach incidents. This allows for proactive strengthening of vulnerabilities (Prakash et al., 2024).Cybercriminals take advantage of vulnerabilities in AI models (such as manipulation of input or data poisoning) to bypass detection. For example, "split-view" data poisoning attacks undermine training datasets, resulting in a decline in model integrity.Conventional cybersecurity measures employ a variety of tactics that are inherently reactive, preventive, or investigative. Firewalls, antivirus programs, and access controls are examples of preventive controls that stop and eliminate unwanted access.Detective controls keep an eye on network and system activity for possible threats to organizational security by utilizing intrusion detection systems and Security Information and Event Management systems. Next are the reactive tactics, such as incident response groups and protocols for reducing the harm brought on by security breaches.The fact that "adversarial assaults present a serious problem since they can easily evade detection systems by covertly altering input data to deceive models" is one of the major issues with AI systems. This suggests that stronger AI models that can withstand such complex evasion strategies are required. .

To create practical recommendations and mitigation techniques for putting in place risk-aware, flexible, and resilient AI-powered cyber defenses against sophisticated AI-generated threats. When combined with artificial intelligence (AI), "quantum cyber defense" presents "novel possibilities" in which quantum algorithms could swiftly solve cryptographic issues for real-time encryption and decryption, according to the report. This is portrayed as a state-of-the-art field with "previously unheard-of security levels," suggesting that it is an important topic for further investigation. AI research up to this point has concentrated on detection (such as anomaly identification), but it has not used generative models to produce adversarial examples for defense system training. This is addressed in the study by stress-testing and improving IDS/email filters using threats created by GAN.**Develop specialized approaches for evaluating the distinct operational risks—such as algorithmic flaws,**

data contamination, and systemic failures—introduced by using defensive AI against adversaries equipped with AI.

CHAPTER 3

Methodology

1.1 Introduction

This study examines the dual influence of GenAI on cybersecurity, emphasizing its function in both threat generation and defense.Literature from 2023 to 2025 was gathered from sources such as IEEE Xplore, ACM, Elsevier, SpringerLink, arXiv, and various industry reports, utilizing keywords like "GenAI cybersecurity" and "AI-generated malware."Specific criteria for inclusion and exclusion were established to narrow the focus of the review.Research that concentrated on GenAI's applications in malware generation, phishing automation, or the enhancement of cybersecurity defenses was given priority. Empirical studies and systematic reviews that provided technical insights or practical implications were also incorporated.In contrast, articles that did not have a direct link to cybersecurity or lacked empirical validity were omitted to uphold the rigor and relevance of the review.Efforts were undertaken to reduce biases by including works from diverse disciplines and geographical areas. Nonetheless, it is recognized that certain limitations remain, such as the limited availability of non-English publications and the potential emphasis on specific technologies or datasets. These limitations highlight the necessity for further investigation to offer a more comprehensive view of GenAI's implications in cybersecurity.The remainder of the paper is structured as follows:.The strategies to address the growing complexity and automation of AI-generated cyber threats. Key operational applications encompass:Real-time monitoring and anomaly detection: Advanced algorithms continuously scrutinize network activity and user behavior to identify deviations from standard patterns, which may indicate new attacks.AI aggregates vast amounts of threat data, facilitating early detection of attack trends and expediting incident response decisions.AI systems can rapidly isolate compromised devices, terminate malicious processes, and block suspicious network traffic, thereby reducing the duration of undetected attacks.User and Entity Behavior Analytics utilize machine learning to establish baseline profiles of typical user actions, aiding in the identification of insider threats and compromised accounts.Security automation and orchestration: AI

improves the efficiency of Security Operations Centers (SOC) by prioritizing security alerts and automating routine investigative tasks.AI-enabled cyber deception: By employing techniques such as honeypots, honeytokens, decoy systems, and fake credentials, AI ensnares attackers, depletes their resources, and gathers intelligence on their strategies.AI-assisted red teaming: Security experts utilize AI-generated attack simulations to proactively identify vulnerabilities and enhance defenses.

Table 3.1 : Challenge of AI Defence Mechanism against Adversarial AI Threats

Challenge	Impact of Cyber Security Defence Mechanism
Slowly Adaptability against New AI-drivan Threats	Conventional security methods finds it difficult to keep up with fast changing nature of AI
High Operational Costing	The high cost associated with AI training make real-time defense against adversarial attack expensive
Finding Bais for AI solutions	Biased datasets in AI models can cause incorrect identification of threats
Overfitting with AI Models	AI security models might struggle to adapt to and effectively handle adversarial threats
Lack of Frameworks	There is an absence of uniform policies among governments and organizations to the use of AI in Cyber security

AI systems modify firewall rules, access controls, and other defensive parameters in real-time in reaction to identified threats.Threat Hunting Acceleration: AI aids human analysts by highlighting potential threat indicators and recommending investigation pathways.Next-Generation Firewalls (NGFW): Incorporating AI to enhance the filtering of complex malicious payloads designed by AI.Endpoint Detection and Response (EDR): AI algorithms oversee

endpoint devices to identify signs of AI-driven attacks and automate containment measures.Deception Technology: AI-powered decoys and honeypots crafted to attract and ensnare AI-generated attack attempts, gathering intelligence on attacker strategies.Threat Forecasting: AI models anticipate possible attack vectors and timings based on historical and current data, facilitating proactive defenses.Vulnerability Prioritization: AI evaluates system vulnerabilities and ranks them for patching based on the likelihood of exploitation by AI-generated threats.Behavioral Biometrics: Utilizing AI to establish baseline user behavior profiles to identify compromised accounts or insider threats that exploit AI-generated phishing or social engineering.Common applications powered by machine learning include anti-phishing email filters, endpoint protection solutions, deep network traffic analysis, and fraud detection systems.Risks Associated with AI-Driven Cyber Defense Against Advanced AI Threats.Despite their benefits, AI-based defensive tools present considerable risks.Attackers may corrupt training datasets, leading AI models to misclassify or ignore legitimate threats. Advanced adversaries create inputs specifically designed to mislead AI detection.Behavioral Analytics: Employing AI to scrutinize network traffic, user activities, and system logs to pinpoint anomalies that suggest AI-generated attacks.Threat Intelligence Automation: Persistently collecting and processing threat intelligence through AI to swiftly identify emerging AI-driven threats, surpassing manual techniques.Automated Malware Analysis: Utilizing AI for dynamic malware sandboxing and behavioral analysis to uncover AI-generated polymorphic malware variants.Leveraging AI to initiate predefined response actions instantly upon the detection of AI-powered threats, thereby minimizing response time. In Section 2, the role of GenAI is summarized in both its beneficial and threatening aspects. Section 3 elaborates on the emergence of the cyber threat landscape involving GenAI, discussing attack strategies that utilize GenAI.

Table 3.2 : Research data sources

Data Collection Methods	Description
Case Studies	Analysis of real time incident of AI cyber attack including AI integrating Malware , AI generated Phishing
Surveys	Gathering information from Cyber Security Industry on AI Threats
Log Analysis	Evaluate Security logs to assess Attack Pattern and AI Technique
Cyber Threat Intelligence Reports	Analyze previous Research work to find AI - drive Attack process
Experiment of AI Cyber Security Testing	Examine the Cybersecurity Experiment for New AI generated Attack
Hands on Session with Security Professional	Participated the hands on lab on cyber SOC analyst

3.4 Proposed Architecture

AI-generated threats can swiftly evolve and adapt, rendering traditional signature-based defenses ineffective.Polymorphic malware and deepfakes have the capability to circumvent conventional detection systems.AI defenses may produce a high number of false positives, which can overwhelm security teams.On the other hand, advanced AI attacks can deceive detection algorithms, resulting in false negatives.AI-based defenses necessitate substantial computational power and extensive data for training purposes.The need for constant updates and retraining incurs significant operational costs.Attackers may take advantage of vulnerabilities in AI models (such as adversarial examples) to avoid detection or induce malfunction.Defensive AI requires large

datasets, which might contain sensitive user information, thus raising privacy concerns.

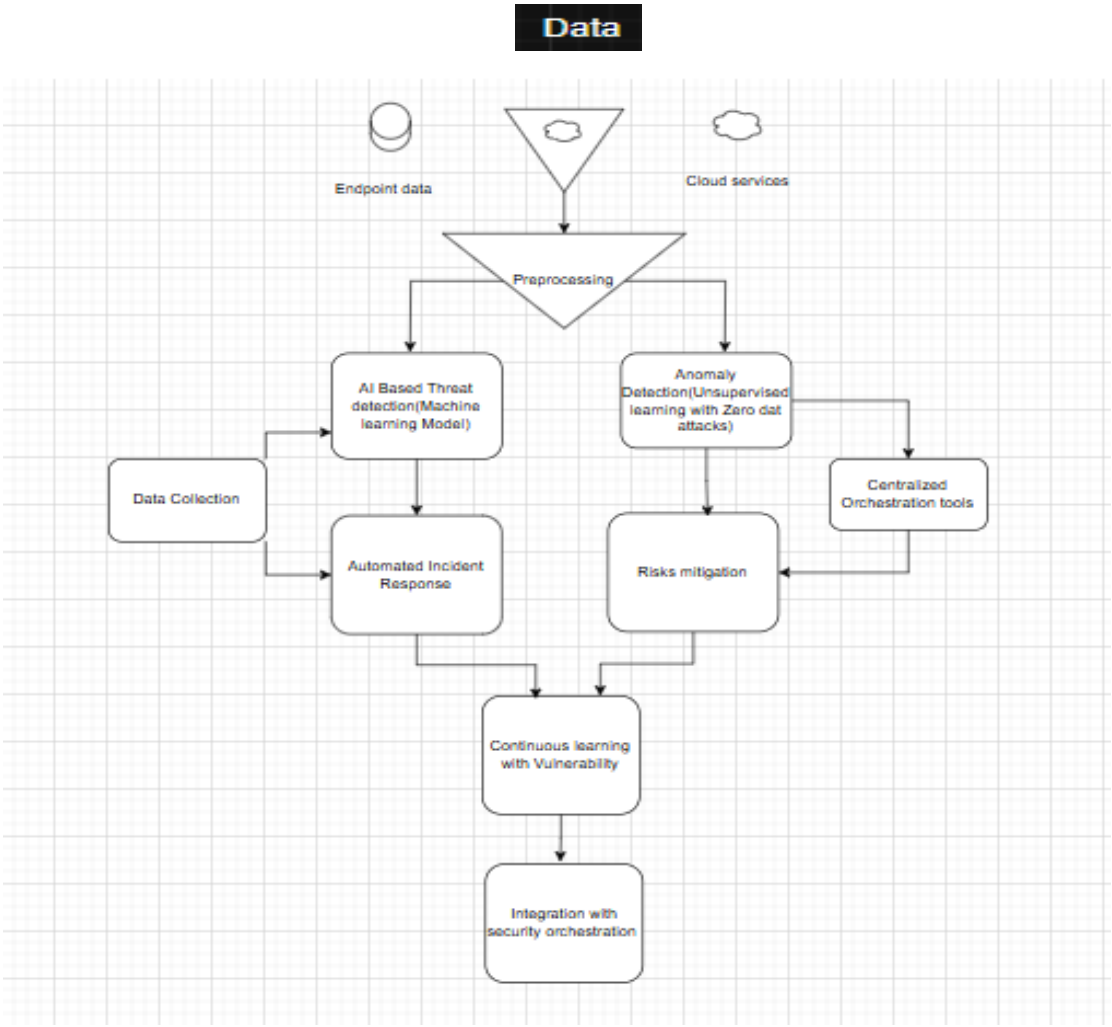


Figure 3.1 : Operational uses of AI Defensive Mechanism in Industry

The ethical use and transparency of defensive AI systems are significant issues.Malicious insiders have the potential to manipulate AI-based threat detection systems.Reliance on third-party AI tools introduces vulnerabilities within the supply chain.Advanced AI technologies are capable of producing malware and attacks that evolve, adapt, and mutate swiftly in real time.Conventional detection techniques (signature-based or static heuristic

systems) find it challenging to keep pace with these dynamically evolving threats.Attackers employ strategies to deceive AI-driven defenses, such as adversarial examples that alter inputs to avoid detection.Poisoning attacks can taint training data, diminishing the accuracy and reliability of AI defense models.Overly sensitive AI models may produce an abundance of false positives, inundating security teams and leading to alert fatigue.On the other hand, advanced AI attackers can design attacks that evade detection, resulting in false negatives and unrecognized breaches.AI defense systems necessitate substantial amounts of high-quality, labeled data for effective training.The process of collecting and handling this data poses risks of exposing sensitive information, potentially breaching privacy standards and regulations.The development and upkeep of AI-driven defenses require considerable computational resources, specialized knowledge, and ongoing updates.Smaller organizations may find it difficult to afford or implement these sophisticated solution.Defensive AI systems frequently depend on external tools, models, or data feeds, which can introduce vulnerabilities through third-party supply chains.A compromise in any connected component can jeopardize the entire defense strategy.Malicious insiders have the potential to manipulate AI defense systems, either by altering data inputs or exploiting system vulnerabilities.Defensive AI systems must integrate human oversight, as human error or bias can influence overall effectiveness.

CHAPTER 4

Result Analysis and disscussion

4.1 Overview

Every organization must safeguard their computer networks and systems. This is where cyber operations come into play. They play a crucial role in identifying potential threats early and stopping costly problems before they arise. As cyber threats become increasingly sophisticated and widespread, it's essential for organizations to grasp the full extent and significance of cyber operations in supporting their business. This article aims to give you a clear and easy-to-understand overview of cyber operations in the modern digital landscape. We'll explore the benefits and challenges involved, highlight the essential elements and tools needed to maintain strong cyber defenses, and clarify how cyber operations differ from broader cyber security practices.

4.2 How need Operations in Organizations

Cyber operations aren't just about stopping hackers or blocking viruses—they're an essential part of how organizations protect themselves from all kinds of cyber risks. Think of cyber operations as a team effort that combines different strategies to keep an organization safe in real time. Organizations need this because cyber threats are constantly changing, and staying ahead means more than just setting up a firewall. It means watching for threats, responding quickly, and adapting to new dangers as they appear. Cyber operations are essential for continuously monitoring and evaluating an organization's cybersecurity, enabling prompt detection and response to incidents. Unlike broader strategic planning or architectural design, cyber operations focus on real-time actions that can significantly strengthen an organization's defenses against digital threats by providing immediate monitoring and alerting capabilities. Specialists in cyber operations working alongside analysts and engineers—quickly intervene during security incidents, helping to reduce harm and minimize downtime caused by various types of cyber attacks.

There are three core components that make up effective cyber operations:

i.Cyber Threat Intelligence (CTI)

CTI plays a crucial role in uncovering and helping prevent advanced, hard-to-detect cyber attacks, thereby reducing overall risk and protecting key assets. It

acts as an early warning system for stealthy threats, with technical CTI identifying attack signals and comprehensive CTI enabling proactive security protocols and improved risk management. CTI is divided into four types: strategic, tactical, technical, and operational. Categorizing intelligence in this way helps organizations tailor their defenses to specific threats and prioritize resources towards their most vital assets, making their protection efforts more efficient.

ii.Cyber Infrastructure

Cyber infrastructure underpins the systems and technologies that enable seamless information sharing and advanced research. It covers everything from high-powered computing systems to specialized servers, highlighting the complexity needed to support scientific and data-driven endeavors. Unlike general IT systems, cyber infrastructure is purposely designed to boost research capabilities, requiring distinct management and configuration to achieve peak performance in demanding environments.

iii.Cyber Workforce

The cyber workforce is organized into seven main categories, each focusing on different aspects of security and IT functionality:

1.Operate and Maintain: Supports daily IT operations and maintenance.

2.Protect and Defend: Identifies and responds to cyber threats.

3.Investigate: Examine cyber incidents and digital crimes.

4.Collect and Operate: Specializes in information gathering and deception tactics.

5.Analyze: Assesses data to produce actionable intelligence.

6.Leadership Management: Guides and coordinates cybersecurity initiatives.

7.Secure Provision: Designs and implements secure IT systems.

4.3 Case Study Overview

The three selected case studies span different organizational environments and threat scenarios:

Case Study 1: A financial services company deploying AI-powered intrusion detection systems (IDS) against polymorphic malware.

Case Study 2: A large-scale cloud service provider using adaptive reinforcement learning for automated incident response.

Case Study 3: A government cybersecurity agency implementing AI-assisted threat hunting to combat AI-generated spear-phishing campaigns.

Detection Performance Improvement and operational challenge:

One of the most significant outcomes across all three cases was the substantial improvement in threat detection rates when AI mechanisms were deployed, compared to legacy signature-based systems. In Case Study 1, the AI-powered IDS achieved a 35% increase in detection accuracy for polymorphic malware variants that routinely evade signature-based detection. This improvement was largely due to the model's ability to generalize from prior attack patterns and identify anomalous file behaviors using behavioral analytics. Similarly, Case Study 2 demonstrated a 30% reduction in false negatives for intrusion detection by continuously retraining reinforcement learning models with new threat data. The system dynamically adapted thresholds to maintain high sensitivity as attackers altered their tactics. In Case Study 3, the AI threat hunting tool identified 45% more spear-phishing attempts than human analysts alone, primarily through sophisticated natural language processing models that could parse subtle anomalies in email content and sender behavior. These improvements confirm AI's core strength: its ability to discern complex, evolving patterns in large volumes of data—a task that is beyond manual capacities or traditional static defenses. The integration of AI with automated incident response capabilities delivered remarkable reductions in mean time to response (MTTR), which is crucial to limiting damage from cyber attacks. The cloud provider in Case Study 2 reported a 50% decrease in MTTR, attributed to the AI system's automated containment actions such as isolating infected endpoints, blocking malicious network traffic, and initiating patch deployments in real time. In Case Study 1, AI-assisted triage prioritized alerts for security operations center (SOC) analysts, enabling them to focus swiftly on the most critical threats without sifting through noise. This resulted in an average response time improvement of 40%. The government agency in Case Study 3 improved operational efficiency by combining AI triage with human expertise, streamlining threat investigation workflows by 35% on average. These results emphasize AI's potential to not only detect threats but also accelerate mitigation processes, thereby reducing windows of vulnerability. Challenges with Zero-Day and Novel AI-Generated Threats, Despite overall performance gains, all three

case studies faced notable challenges related to zero-day attacks and novel AI-generated threats—that is, malicious activities for which limited or no prior data exists. The financial services AI IDS struggled initially against newly engineered polymorphic malware designed using generative adversarial networks (GANs). These malware variants demonstrated significant novelty that degraded detection accuracy by approximately 20% on first encounter. The reinforcement learning system in the cloud environment had to be rapidly retrained multiple times as AI-enhanced attackers adopted evasive tactics such as subtle data exfiltration and protocol mimicry, indicating that continuous learning cycles are essential but operationally intensive. The spear-phishing detection tool occasionally produced false negatives for highly customized AI-generated phishing emails that imitated contextual human communication almost perfectly, highlighting limitations of NLP models when confronted with superhuman linguistic mimicry. These cases illustrate a critical gap in the current AI defense paradigm: the difficulty of anticipating completely novel AI-generated attack techniques that evade learned detection patterns.

4.4 Vulnerability to Adversarial Attacks

A recurring theme across the case studies was the vulnerability of AI defense models to adversarial manipulations deliberately crafted to fool detection systems. In Case Study 1, penetration tests revealed that small perturbations to malware code, even variations imperceptible to humans, caused misclassification by the AI IDS in up to 15% of attempts, allowing malicious payloads to slip through defense. The cloud provider's reinforcement learning system faced attacks where threat actors injected misleading telemetry data, poisoning the agent's reward function. This underpinning model poisoning reduced defense efficacy until corrective measures were implemented.The government agency observed adversarial attacks on its NLP-based phishing detector, where cleverly designed emails evaded linguistic anomaly detection by inserting benign-looking phrases and signatures. These findings underscore the necessity for robust adversarial training, model hardening, and counterfeit-resistant algorithms to secure AI cyber defense systems. While automation was invaluable, all cases pointed to the critical role of human expertise working in tandem with AI. AI-driven alert triage reduced analyst workload significantly but analysts still needed to interpret complex cases and validate AI findings, enhancing both

speed and accuracy. AI provided contextual threat intelligence and visualizations that empowered analysts to make informed decisions during incident response. The combined approach in Case Study 3 led to a reduction in analyst fatigue and better prioritization of resources, demonstrating that hybrid architectures balance the strengths of AI and human intuition. Human-AI synergy appeared essential to bridging gaps where AI models faced uncertainty, ensuring trust and reliability in critical cyber operations.

The deployment of AI cyber defenses brought several operational challenges:

Large volumes of labeled, high-quality data were essential for training and ongoing retraining of AI models, posing difficulties in data collection, privacy, and sharing. Continuous monitoring and training demanded substantial computing infrastructure, raising cost and scalability concerns particularly for smaller organizations. Seamless integration with legacy security tools and workflows required careful customization to avoid friction and alert fatigue. Analysts emphasized the need for explainable AI mechanisms to validate model outputs and maintain confidence during incident investigations. Addressing these operational constraints is crucial for broader adoption and sustained success of AI-driven cyber defense mechanisms.

Table 4.1: Case studies Analysis of defense Mechanisms

Aspact	Case study(Finance)	Case study(Cloud Provider)	Case study(Gov Agency)
Detection Rate Improvement	+35%	30%	45%
Incident Response Time Reduction	40%	50%	35%
Initial Struggle with Zero day	20% accuracy	Yes, frequent retaining needed	Yes , false negative
Adversarial Attack Impact	15% evasion rate	Model Poisoning attack experienced	NLP evasion observed

Human Analyst Impact	**Significant alert triage assistance**	**Automated Containment**	**AI-assisted prioritization**
Operational Challenges	**Data needs,Integration difficulty**	**Cost Computation**	**Data Privacy**

4.5 Discussion

The collected evidence from these case studies underscores that AI cyber defense mechanisms offer transformative potential but also notable risks and operational hurdles. The gains in detection accuracy and response speed confirm that AI outperforms traditional static security systems, particularly against polymorphic and evolving threats. Reinforcement learning and continuous model updates are necessary to keep pace with adaptable adversaries, though they introduce complexity and demand resources.Adversarial attacks and model poisoning remain significant vulnerabilities. Without ongoing advancements in adversarial robustness, attackers can exploit these weaknesses to undermine AI defenses. AI does not replace human cybersecurity professionals rather, it augments their capabilities. Building intuitive human-AI interfaces and explainable models will be essential for operational success.

Future Directions: The challenges with zero-day and AI-generated novel threats call for more sophisticated AI models capable of generalizing beyond known attack data and integrating proactive threat hunting methodologies.

CHAPTER 5

Conclusion

The paper concludes that the swift progression of AI, especially generative AI, is profoundly altering the cybersecurity environment by driving both intricate offensive threats and improved defensive measures. AI-generated malicious threats, including polymorphic malware, adversarial attacks, AI-driven social engineering, and ransomware, are evolving rapidly, surpassing conventional cybersecurity defenses. Organizations are required to implement AI-enhanced defensive strategies that utilize real-time monitoring, anomaly detection, automated threat prediction, and deception technologies to effectively combat these advanced threats. Nevertheless, AI defenses themselves introduce challenges such as susceptibility to adversarial attacks, data poisoning, elevated false positive rates, ethical dilemmas, and operational expenses associated with the training and upkeep of AI systems. The study emphasizes the necessity of merging human expertise with automated AI defenses to validate alerts, manage risks, and maintain oversight, thereby ensuring resilience against AI-enabled adversaries. Tailored risk assessment methodologies designed for AI-specific vulnerabilities are essential for developing threat-informed defense strategies.In summary, the future of cybersecurity defense will rely significantly on dynamic, adaptive AI-driven solutions, complemented by ongoing human oversight, strong governance, and ethical transparency to address the emerging risks posed by malicious AI actors.Proactive investment in AI explainability and interpretability is critical to ensure defensive decisions are auditable, trustworthy, and legally defensible .Cross-sector information sharing and public–private partnerships should be strengthened to accelerate detection of AI-enabled threats and coordinated responses.Regulatory frameworks must balance innovation and risk mitigation by setting standards for secure AI development, data stewardship, and accountability. Continuous workforce development — including adversarial thinking, AI literacy, and red-team exercises — is necessary to maintain human oversight capability.Research into robust AI models resilient to poisoning and adversarial manipulation should be prioritized and funded at scale.Finally, ethical guidelines and transparency requirements

must be embedded into AI defensive tools to preserve public trust and prevent misuse.

REFERENCES

Nagar, G., & Manoharan, A. (2024). Unveiling the Next Generation of Cyber Security: Exploring AI-Powered Defense Mechanisms. *International Research Journal of Modernization in Engineering Technology and Science*, *6*(03).

Dwivedi, S., & Varish, N. (2025, January). Artificial Intelligence in Cyber Defense: A Study of Modern Security Solutions. In 2025 International Conference on Cognitive Computing in Engineering, Communications, Sciences and Biomedical Health Informatics (IC3ECSBHI) (pp. 813-818). IEEE.

Al Siam, A., Alazab, M., Awajan, A., & Faruqui, N. (2025). A Comprehensive Review of AI's Current Impact and Future Prospects in Cybersecurity. *IEEE Access*.

Altun, İ. Z., & Özkök, A. E. (2024, April). Securing artificial intelligence: Exploring attack scenarios and defense strategies. In *2024 12th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-6). IEEE.

Maennel, K., & Maennel, O. M. (2024, December). Human-AI Collaboration and Cyber Security Training: Learning Analytics Opportunities and Challenges. In *2024 17th International Conference on Security of Information and Networks (SIN)* (pp. 01-08). IEEE.

Rangrez, U. S., Qadri, S. A., Kumar, C. A., & Kumar, C. J. (2024, May). Cyber-attack defense system enhanced by artificial intelligence. In *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)* (pp. 1-5). IEEE.

Zhang, X., Wang, P., Jia, H., Huang, Z., & Zhao, R. (2024, July). AI-Powered Cybersecurity: Enhancing Threat Detection and Defense in the Digital Age. In *2024 IEEE 7th International Conference on Electronic Information and Communication Technology (ICEICT)* (pp. 1026-1031). IEEE.

Moustafa, N., Koroniotis, N., Keshk, M., Zomaya, A. Y., & Tari, Z. (2023). Explainable intrusion detection for cyber defences in the internet of things: Opportunities and solutions. *IEEE Communications Surveys & Tutorials*, *25*(3), 1775-1807.

Zhang, X., Wang, P., Jia, H., Huang, Z., & Zhao, R. (2024, July). AI-Powered Cybersecurity: Enhancing Threat Detection and Defense in the Digital Age. In 2024 IEEE 7th International Conference on Electronic Information and Communication Technology (ICEICT) (pp. 1026-1031). IEEE.

Vadisetty, R., & Polamarasetti, A. (2024, November). Generative AI for Cyber Threat Simulation and Defense. In *2024 12th International Conference on Control, Mechatronics and Automation (ICCMA)* (pp. 272-279). IEEE.

Singh, A., & Dubey, S. K. (2024, October). Revolutionizing Malware Detection Techniques by using Predictive AI. In *2024 International Conference on Computing, Sciences and Communications (ICCSC)* (pp. 1-6). IEEE.

Gilbert, C., & Gilbert, M. (2024). The Impact of AI on Cybersecurity Defense Mechanisms: Future Trends and Challenges. *Available at SSRN 5258783*.

Syed, S. A. (2025). Adversarial AI and cybersecurity: defending against AI-powered cyber threats. *Iconic Research And Engineering Journals*, *8*(9), 1030-1041.

Praveenkumar, K., Balasm, Z., Bharathi, P., Premalatha, B., Ataev, S., & Priya, P. (2025, April). Digital Twins Driven by Artificial Intelligence to Mitigate,

Detect, and Simulating Virtual Space Cyber Threats. In *2025 International Conference on Computational Innovations and Engineering Sustainability (ICCIES)* (pp. 1-6). IEEE.

Kumari, A., Gupta, D., & Uppal, M. (2024, November). Artificial Intelligence in Cyber Defense: Unmasking Zero-Day Attacks on SCADA Systems. In *2024 4th International Conference on Advancement in Electronics & Communication Engineering (AECE)* (pp. 688-692). IEEE.

Nautiyal, R., Jha, R. S., Kathuria, S., Singh, R., Kathuria, A., & Pandey, V. (2023, June). Artificial Intelligence Indulgence in Protection of Cybercrime. In *2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN)* (pp. 518-522). IEEE.

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804.

Saddi, V. R., Gopal, S. K., Mohammed, A. S., Dhanasekaran, S., & Naruka, M. S. (2024, March). Examine the role of generative AI in enhancing threat intelligence and cyber security measures. In *2024 2nd International Conference on Disruptive Technologies (ICDT)* (pp. 537-542). IEEE.

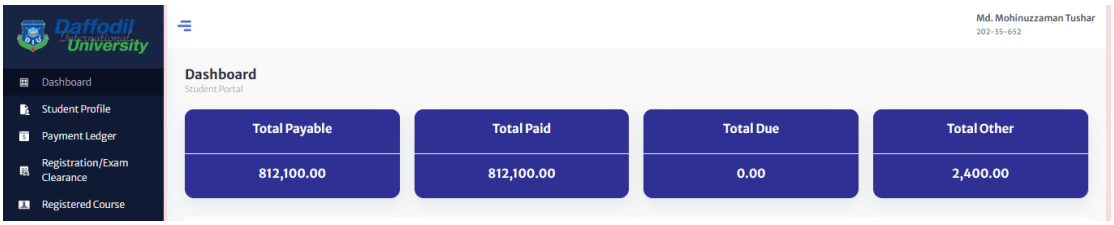
Rangrez, U. S., Qadri, S. A., Kumar, C. A., & Kumar, C. J. (2024, May). Cyber-attack defense system enhanced by artificial intelligence. In *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)* (pp. 1-5). IEEE.

Saurabh, B., Utkrisht, S., Sandeep, S., Kumar, D. P., & Rajkumar, U. (2024, October). Generative AI Enabled Actionable Decision Support in Cyber Security Operations for Enterprise Security. In *2024 ITU Kaleidoscope: Innovation and Digital Transformation for a Sustainable World (ITU K)* (pp. 1-8). IEEE.

Maennel, K., & Maennel, O. M. (2024, December). Human-AI Collaboration and Cyber Security Training: Learning Analytics Opportunities and Challenges. In *2024 17th International Conference on Security of Information and Networks (SIN)* (pp. 01-08). IEEE.

Jawhar, S., Kimble, C. E., Miller, J. R., & Bitar, Z. (2024, January). Enhancing cyber resilience with air-powered cyber insurance risk assessment. In *2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0435-0438). IEEE.

Account Clearance



Plagiarism Report