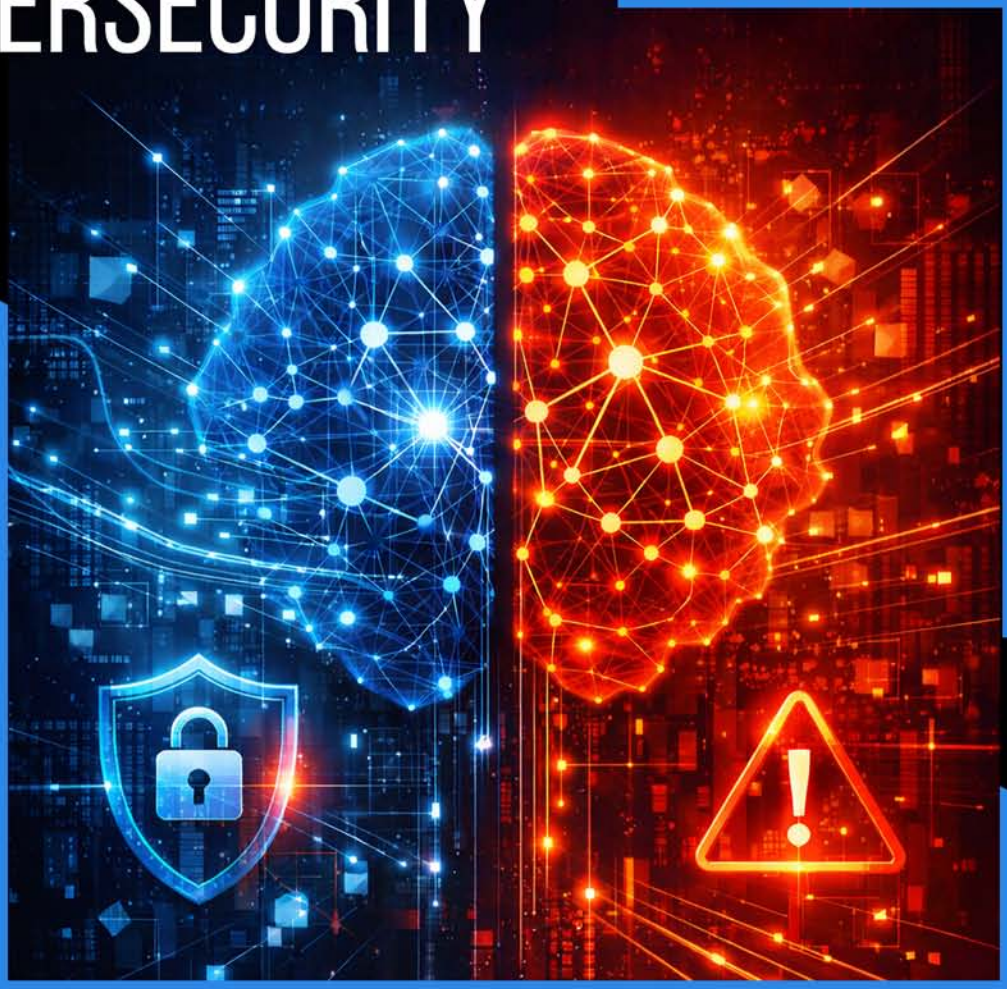
AI-DRIVEN THREAT INTELLIGENCE FRAMEWORKS REVOLUTIONIZING ENTERPRISE CYBERSECURITY



Editors:
Pundru Chandra Shaker Reddy
Yadala Sucharitha
Thillaiarasu Nadesan

Bentham Books

AI-Driven Threat Intelligence Frameworks: Revolutionizing Enterprise Cybersecurity

Edited by

Pundru Chandra Shaker Reddy
Department of Computer Science and Engineering
Amity School of Engineering and Technology
Amity University, Noida
Uttar Pradesh, India

Yadala Sucharitha
Department of Computer Science and Engineering
Sharda School of Engineering and Technology
Sharda University, Greater Noida
Uttar Pradesh, India

&

Thillaiarasu N
School of Computing and Information Technology
REVA University, Bangalore
Karnataka, India

AI-Driven Threat Intelligence Frameworks: Revolutionizing Enterprise Cybersecurity

Editors: Pundru Chandra Shaker Reddy, Yadala Sucharitha & Thillaiarasu N

ISBN (Online): 979-8-89881-384-0

ISBN (Print): 979-8-89881-385-7

ISBN (Paperback): 979-8-89881-386-4

Published by Bentham Science Publishers Pte. Ltd. Singapore, in collaboration with Eureka Conferences, USA.

First published in 2026.

need for a court order if at any point you breach any terms of this License Agreement. In no event will any delay or failure by Bentham Science Publishers in enforcing your compliance with this License Agreement constitute a waiver of any of its rights.

3. You acknowledge that you have read this License Agreement, and agree to be bound by its terms and conditions. To the extent that any other terms and conditions presented on any website of Bentham Science Publishers conflict with, or are inconsistent with, the terms and conditions set out in this License Agreement, you acknowledge that the terms and conditions set out in this License Agreement shall prevail.

Bentham Science Publishers Pte. Ltd.
No. 9 Raffles Place
Office No. 26-01
Singapore 048619
Singapore
Email: subscriptions@benthamscience.net

CONTENTS

FOREWORD

In today's hyperconnected digital era, the landscape of cybersecurity is evolving at an unprecedented pace. The exponential growth of data, the increasing sophistication of cyber threats, and the dynamic nature of enterprise IT infrastructures demand innovative and intelligent defense mechanisms. Amidst this rapid transformation, artificial intelligence (AI) has emerged as a pivotal force, capable of redefining how organizations perceive, predict, and prevent security breaches.

AI-DRIVEN THREAT INTELLIGENCE FRAMEWORKS:

Revolutionizing Enterprise Cybersecurity comes at a critical time when traditional cybersecurity approaches are proving insufficient against agile and adaptive threat actors. This timely volume presents a comprehensive exploration of AI-integrated threat intelligence systems, offering deep insights into how machine learning, natural language processing, and automated reasoning are being harnessed to fortify enterprise defenses.

The contributors to this book□?"comprising eminent researchers, cybersecurity experts, and industry practitioners□?"bring together theoretical foundations, cutting-edge frameworks, and practical applications that illuminate the transformative potential of AI in cybersecurity. From detecting zero-day attacks to automating incident response and enabling proactive threat hunting, the chapters collectively underscore the significance of intelligent systems in securing digital ecosystems.

What sets this book apart is not only its technical depth but also its forward-looking vision. It anticipates the challenges and opportunities that lie ahead, providing readers with both conceptual clarity and actionable strategies. Whether you are a cybersecurity professional, academician, student, or enterprise leader, this book offers invaluable knowledge that can empower your understanding and application of AI in protecting critical digital assets.

As we move toward an increasingly digital future, embracing AI-driven cybersecurity frameworks is not merely an option??"it is an imperative. I commend the editors and authors for their meticulous effort in compiling this insightful volume, which will undoubtedly serve as a cornerstone reference for years to come.

Dr. Vivekanand A
Department of Computer Science and Engineering
CMR College of Engineering and Technology
Hyderabad, India

PREFACE

The digital transformation of the modern enterprise landscape has ushered in an era of boundless opportunities-yet it also brings with it unprecedented challenges in cybersecurity. As organizations increasingly depend on interconnected systems, cloud platforms, and mobile infrastructures, the sophistication, scale, and frequency of cyber threats have risen alarmingly. In this context, the role of Artificial Intelligence (AI) has shifted from a futuristic concept to an indispensable asset in proactive threat detection and response.

This edited volume, ***AI-Driven Threat Intelligence Frameworks: Revolutionizing Enterprise Cybersecurity***, serves as a timely and comprehensive resource that explores how AI technologies are redefining threat intelligence and transforming cybersecurity operations across sectors. It brings together leading scholars, researchers, and practitioners who provide insights into the convergence of AI and cybersecurity, while also addressing the operational, ethical, and strategic considerations in deploying AI-driven frameworks.

The book is structured into twelve thought-provoking chapters, each contributing to a broader understanding of the evolving cybersecurity landscape:

- **Chapter 1** lays the foundation by discussing the broad spectrum of cybersecurity applications, current challenges, and forward-looking directions in the digital age.
- **Chapter 2** introduces fundamental AI concepts, tracing their historical evolution and relevance to modern applications.
- **Chapter 3** bridges the domains of AI and cybersecurity, highlighting synergies, overlaps, and practical implementations.
- **Chapter 4** presents an interdisciplinary perspective on how English language proficiency plays a role in AI-driven cybersecurity settings.
- **Chapter 5** delves into the dynamics of social networks, exploring how AI can be used for cyber threat intelligence and trend prediction, especially in platforms like X.
- **Chapter 6** offers a practical guide to Security Operations Centres (SOC), emphasizing their transformation in the AI era.
- **Chapter 7** focuses on endpoint security, showing the shift from traditional reactive approaches to intelligent, AI-enabled proactive strategies.
- **Chapter 8** explores sentiment analysis in cybersecurity contexts, including applications, datasets, challenges, and future outlooks.
- **Chapter 9** examines the convergence of AI and blockchain, investigating integration feasibility, research gaps, and emerging applications.
- **Chapter 10** introduces a novel framework for managing cybersecurity in Socially Responsible Investment (SRI) funds, balancing ethical compliance with threat mitigation.
- **Chapter 11** investigates security in smart cities, analyzing use cases, technological advancements, challenges, and evolving trends.
- **Chapter 12** concludes with a visionary chapter on the next generation of AI in cybersecurity, addressing upcoming trends and future research directions.

Together, these chapters offer a multidimensional perspective on AI-driven threat intelligence from foundational knowledge to advanced frameworks and practical use cases. The book aims to serve not only as a scholarly reference but also as a practical guide

for professionals, decision-makers, and students navigating the complexities of modern cybersecurity ecosystems.

We extend our sincere gratitude to all the contributing authors and reviewers whose expertise and commitment have enriched this volume. We also acknowledge the support from Bentham Science, whose platform continues to foster meaningful contributions to emerging areas of science and technology.

We hope this book will inspire future research, encourage cross-disciplinary collaboration, and support enterprises in building resilient and intelligent cybersecurity strategies.

Dr. Pundru Chandra Shaker Reddy
Department of Computer Science and Engineering
Amity School of Engineering and Technology
Amity University, Noida
Uttar Pradesh, India

Dr. Yadala Sucharitha
Department of Computer Science and Engineering
Sharda School of Engineering and Technology
Sharda University, Greater Noida
Uttar Pradesh, India

Dr. Thillaiarasu N
School of Computing and Information Technology
REVA University, Bangalore
Karnataka, India

List of Contributors

Amdewar Godavari	Department of CSE (Networks), Kakatiya Institute of Technology and Science, Warangal, India
Ambati Suvarna	School of Business, SR University, Warangal, India
C Dastagiraiah	Department of CSE, Anurag University, Hyderabad, India
C Santhosh Kumar	Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India
Diivyaam Shah	Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, India
D Chitra	Department of MBA, Panimalar Engineering College, Chennai, India
Gousiya Begum	Department of CSE, Mahatma Gandhi Institute of Technology, Hyderabad, India
Goddumarri Suryanarayana	Symbiosis Institute of Technology, Hyderabad Campus, Symbiosis International University, Hyderabad, India
K Madhan	Department of Information Technology, St. Joseph's College of Engineering, Chennai, Tamil Nadu, India
Kisara Rishitha	Department of CSE, BVRIT HYDERABAD College of Engineering for Women, Hyderabad, India
Kiran Dodiya	Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, India
Kapil Kumar	Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, India
Karibasappa Chatrapathi	School of Computing & Information Technology, REVA University, Bangalore, India
Kafila	School of Business, SR University, Warangal, India
K Venkatesh	Department of Engineering in Internetworking, Dalhousie University, Halifax, Canada
K Chatrapathy	School of Computing & Information Technology, REVA University Bangalore, Karnataka, India
LNC Prakash Koratamaddi	Department of Computer Science & Engineering-Data Science, CVR College of Engineering, Hyderabad, India
Lakshmi Hassan Nagaraja	Department of CSE (AI&ML), CVR College of Engineering, Hyderabad, India
Mudarakola Lakshmi Prasad	Computer Science and Engineering, Institute of Aeronautical Engineering, Dundigal, India
M Indrasenareddy	Computer Science and Engineering, BVRIT HYDERABAD College, of Engineering for Women, Hyderabad, India
M Lakshmi Prasad	Computer Science and Engineering, Institute of Aeronautical Engineering, Hyderabad, India

Medikonda Asha Kiran	Department of Information Technology, School of Engineering, Anurag University, Hyderabad, India
Manyam Thaile	Department of Information Technology, School of Engineering, Anurag University, Hyderabad, India
N Gurusamy	Department of AI and DS, Sri Shanmugha College of Engineering and Technology, Sangakiri Salem, Tamil Nadu, India
N Shanmugapriya	Department of Computer Science and Engineering, Dhanalakshmi Srinivasan University, Tamil Nadu, India
Nikita Gaur	School of Computer Science & AI, SR University, Warangal 506371, India
Niteesha Sharma	Department of Information Technology, School of Engineering, Anurag University, Hyderabad, India
Pundru Chandra Shaker Reddy	Amity School of Engineering and Technology Department of Computer Science and Engineering, Amity University, Noida, India
P Esaiarasi	Department of Electronics and Communication Engineering, Mailam Engineering College, Mailam, Tamil Nadu, India
Peddada Nagamani	Department of Information Technology, School of Engineering, Anurag University, Hyderabad, India
Rafath Samrin	Department of Computer Science, College of Computer Science, King Khalid University, Asir-Abha, Saudi Arabia
Ranjit Kumar Elamadurthi	Department of English, Vardhaman College of Engineering, Hyderabad, India
Rayapati Venkata Sudhakar	Department of Computer Science and Engineering, Geethanjali College of Engineering and Technology, Hyderabad, India
Ramesh Babu Pittala	Department of Information Technology, School of Engineering, Anurag University, Hyderabad, India
Sudhanshu Kumar Jha	Department of Electronics and Communication, Faculty of Science, University of Allahabad, Uttar Pradesh, India
Seema Nagaraj	Department of MCA, Bangalore Institute of Technology, Bengaluru, India
Sri Rekha Uppuluri	School of Computer Science & AI, SR University, Warangal, India
Sasanko Sekhar Gantayat	School of Computer Science & AI, SR University, Warangal, India
S Nancy Lima Christy	Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India
Sridhar Chintala	School of Computer Science & AI, SR University, Warangal 506371, India
Sridhar N Koka	Faculty of Business Administration, Panyapiwat Institute of Management, Pak Kret, Thailand
S Yuvalatha	Department of Computer Science and Business Systems, Bannari Amman Institute of Technology, Erode, India
Thinagaran Perumal	Department of Computer Science, University Putra Malaysia, Serdang, Malaysia

Vijay Bhanudas Gujar	Department of Computer Science and Engineering, Arvind Gavali College of Engineering, Satara, India
Vidyullatha Sukhavasi	Department of CSE, BVRIT HYDERABAD College of Engineering for Women, Hyderabad, India
Yadala Sucharitha	Sharda School of Computing Science and Engineering , Department of CSE, Sharda University, Greater Noida, India

CHAPTER 1

Cybersecurity in the Digital Age: Applications, Opportunities, Challenges, and Future Directions

Amdewar Godavari[1,*], Gousiya Begum[2], Rafath Samrin[3], Vijay Bhanudas Gujar[4], C Dastagiraiah[5] and **Sudhanshu Kumar Jha[6]**

[1] *Department of CSE (Networks), Kakatiya Institute of Technology and Science, Warangal, Telangana, India*

[2] *Department of CSE, Mahatma Gandhi Institute of Technology, Hyderabad, Telangana, India*

[3] *Department of Computer Science, College of Computer Science, King Khalid University, Asir-Abha, Saudi Arabia*

[4] *Department of Computer Science and Engineering, Arvind Gavali College of Engineering, Satara, Maharashtra, India*

[5] *Department of CSE, Anurag University, Hyderabad, Telangana, India*

[6] *Department of Electronics and Communication, Faculty of Science, University of Allahabad, Uttar Pradesh, India*

Abstract: Protecting people, businesses, and governments from the plethora of cyber dangers has made cybersecurity a top priority in today's highly linked digital world. In this research paper, we take a close look at cybersecurity in the modern day, analyzing potential risks and discussing ways to mitigate them. In this chapter, we'll take a look at cybersecurity from a high level, covering topics such as its significance, typical vulnerabilities and attacks, successful prevention techniques, and upcoming trends. Everything from private customer information to mission-critical company assets is abundant in today's digital age. With the proliferation of both data and connections, cybersecurity is now more important than ever. Data theft and loss, as well as the availability and integrity of digital systems, can be prevented with effective cybersecurity solutions. Legal responsibilities and regulatory fines may amplify the effects of cyberattacks, which already cause substantial financial losses, harm to reputations, and interruptions to operations. Standard cyber risks and Internet of Things security holes. We performed a comprehensive review to find out what the newest cybersecurity trends, problems, and opportunities are so we can stay ahead of the game. We also talk about where cybersecurity is going in the future, outlining potential tactics for dealing with the ever-changing landscape of cyber threats, new trends, and technological advancements like ML and AI for automated threat detection and response.

[*] **Corresponding Author Amdewar Godavari**: Department of CSE (Networks), Kakatiya Institute of Technology and Science, Warangal, Telangana, India; E-mail: godavariamdewar@gmail.com

Pundru Chandra Shaker Reddy, Yadala Sucharitha, & Thillaiarasu N (Eds.)

Keywords: Artificial intelligence, Cyber resilience, Cyber threats, Cyber-attacks, Cybersecurity, Defense strategies, Digital transformation, Machine learning.

INTRODUCTION

Cyberspace is expanding at a dizzying rate right now. There has been a growing consensus among academics that it is crucial to teach the next generation about cybersecurity principles in light of the ever-changing nature and prevalence of cyber threats. Negligence in cybersecurity and a lack of client knowledge lead to cybercrimes [1]. Recent studies have shown that the United States is the first country to implement threat intelligence frameworks. Nearly 70 countries have included cyber/information security strategies and major legislative measures in their military and national security plans to deal with this problem. Preparation for vulnerabilities, as outlined in the cyber network guide, involves exchanging information about potential dangers in a timely manner; this can help safeguard the environment, businesses, and infrastructure, as well as provide insight into current events. Recent research has used a broad definition of cybersecurity (ISO, 2018) [2]. In their draft, the International Telecommunications Union (ITU) also defines cybersecurity (ITU-T X.1205). Thus, cybersecurity, in its broadest sense, aids in risk management by preventing cyber assaults and data breaches [3].

More complex, targeted, and deadly cybercrimes and hostile actions have emerged in modern times, thanks to scientific progress. A ransomware attack was causing damage to the Atlanta City government and other previous cyber intrusions; this was discovered earlier in 2018. There is now an abundance of private data due to the way the digital revolution has altered our daily lives and the way we do business. Data types include sensitive personal information (such as SSNs and bank account details) and vital company information (such as proprietary systems and intellectual property) [4]. Cybersecurity has risen to the forefront of everyone's agenda due to the increased likelihood of cyber threats caused by the widespread use of digital technologies. Ensuring the availability and integrity of digital systems is an integral part of cybersecurity, which goes beyond simply preventing data theft or loss. The repercussions of a successful cyber assault can be devastating, including not only financial loss but also harm to one's reputation and the interruption of operations. Significant legal liabilities and regulatory fines can result from data breaches for corporations [5]. Both the stakes and the environment are dynamic and ever-changing. The sophistication of cyber-attacks is on the rise, as are the methods used by attackers to circumvent security measures. This means that cybersecurity is an ever-evolving discipline. This article explores the fundamentals of cybersecurity, including why it's important, what kinds of dangers are most prevalent, how to stay safe online, and what trends will shape digital security in the future [6].

Importance of Cybersecurity

Cyberattacks are becoming more common and more damaging, highlighting the need for better cybersecurity. Data privacy, operational continuity, and the protection of sensitive information all depend on robust cybersecurity measures. Having insufficient cybersecurity measures in place might have serious repercussions in this day and age of frequent data breaches and ransomware attacks. Not only can these breaches cause immediate damage, but they can also have long-term consequences, including lost business, legal expenditures, and regulatory fines, which can add up to a catastrophic financial impact [7].

For instance, consumer trust can be severely damaged by data breaches. Identity fraud, financial fraud, and other major consequences can result from the exposure of personal information. Businesses risk serious harm to their reputations when consumers lose faith in their data security measures after a data breach. Reduced consumer loyalty, lost business, and a weakened competitive edge are all possible outcomes of this trust erosion [8]. The increasing sophistication of phishing schemes—which employ misleading emails or websites to coerce consumers into divulging personal information—further emphasizes the importance of robust cybersecurity protocols. Significant financial losses and data breaches can arise because of phishing attempts, which take advantage of human vulnerabilities [9].

The expansion of the Internet of Things (IoT) and linked gadgets has also brought about new security holes. An attacker could potentially gain access to your system through any of your linked devices. If we care about keeping sensitive information safe and avoiding illegal access, we must make sure these devices and the networks they connect to are secure. With more and more of our daily lives taking place online, cybersecurity has become an essential part of contemporary existence [10]. To be effective, cybersecurity must focus on both the prevention of assaults and the development of resilient systems capable of withstanding and recovering from such attacks. Cybersecurity must be a top priority for all organizations and individuals who value their digital assets, privacy, and the security of their operations. Cybersecurity protects IoT devices by preventing unauthorized access, data breaches, and attacks that exploit device vulnerabilities. It ensures secure communication, device authentication, and data integrity, thereby maintaining the reliability and privacy of interconnected IoT systems.

AI-enabled Security Models

AI-enabled security models leverage artificial intelligence techniques such as machine learning, deep learning, and anomaly detection to enhance cybersecurity by identifying, predicting, and mitigating threats in real time. These models can analyze vast amounts of network data, detect unusual patterns, and adapt to

CHAPTER 2

Introduction to AI: Concepts, History, and Applications

Vidyullatha Sukhavasi[1], Kisara Rishitha[1] and **Yadala Sucharitha[2,*]**

[1] *Department of CSE, BVRIT HYDERABAD College of Engineering for Women, Hyderabad, Telangana, India*

[2] *Sharda School of Computing Science and Engineering , Department of CSE, Sharda University, Greater Noida, Uttar Pradesh, India*

Abstract: Artificial Intelligence (AI) is perhaps the most revolutionary technology today, driving innovation across sectors, transforming economies, and impacting daily life. This chapter gives an overview of AI, discussing its core concepts, historical development, and major applications. It starts by explaining AI and separating it from its associated disciplines, like machine learning and data science. The chapter further discusses the basic techniques and strategies in AI, such as rule-based systems, neural networks, and natural language processing. Through the exploration of how AI systems are constructed and trained to do things like speech recognition, image processing, and decision-making, the chapter illuminates the underlying mechanics of AI technology. This chapter gives readers a sound grasp of the fundamental principles of AI, what it can currently do, and what challenges and opportunities it is likely to offer. For business, healthcare, education, and security, AI will be instrumental in the future, and so it is vital to comprehend its changing landscape.

Keywords: Artificial Intelligence (AI), Autonomous Systems, Computer Vision, Deep Learning, Ethical AI, Explainable AI (XAI), Federated Learning, Intelligent Systems, Machine Learning (ML), Natural Language Processing, Neural Networks, Predictive Analytics, Quantum AI, Reinforcement Learning, Robotics, Smart Automation, Supervised Learning.

INTRODUCTION

The goal of Artificial Intelligence (AI), a revolutionary technology, is to create machines that can reason, learn, perceive, and make decisions in order to mimic human intelligence. This chapter's main goal is to give readers an understanding of Artificial Intelligence (AI), including its core concepts, scientific foundations,

[*] **Corresponding Author Yadala Sucharitha:** Sharda School of Computing Science and Engineering , Department of CSE, Sharda University, Greater Noida, Uttar Pradesh, India; E-mail: suchi.yadala@gmail.com

Pundru Chandra Shaker Reddy, Yadala Sucharitha, & Thillaiarasu N (Eds.)

practical applications, and societal consequences. The main focus is on how AI has developed from theoretical concepts to real-world applications in various industries. The chapter places Artificial Intelligence (AI) in the larger context of developing technologies and identifies both the advantages and disadvantages of its adoption by providing a well-organized analysis.

AI-Driven Threat Intelligence Frameworks: Revolutionizing Enterprise Cybersecurity

The recreation of human intelligence by machines, particularly computer systems, is known as Artificial Intelligence (AI). They are designed to perform functions including knowledge acquisition, problem-solving, perception, and understanding of languages that normally need human intellect [1], shown in Table **1**. AI systems are typically faster and more accurate than humans, can learn from information, and get better over time.

Table 1. Comparison of AI and human intelligence.

Aspect	Artificial Intelligence	Human Intelligence
Memory	Large storage capacity and speedy retrieval	restricted and prone to forgetting
Learning	Statistical models that are driven by data	Contextual and experience-based
Speed	Quick, simultaneous processing	Slow, step-by-step analysis
Emotional Intelligence	Absent or rudimentary	Relationships, feelings, and empathy
Adaptability	Constrained by context, retraining is necessary	Extremely adaptable and perceptive
Decision Making	Knowledge and reasoning based on rules	Knowledge, feeling, and perception
Creativity	Creativity based on patterns and rules	Innovative, Perceptive, and Creative

John McCarthy provided one of the first definitions of Artificial Intelligence, defining it as “the science and engineering of making intelligent machines” [2]. AI encompasses a wide range of methods and strategies, including deep learning, machine learning, and rule-based systems. Everyday applications of AI include voice recognition in smartphones, driverless cars, and digital platform content recommendations.

Why AI Matters in the Modern World?

AI is rapidly reshaping how we live, work, and interact. In the digital era, data is generated at an unprecedented scale. AI leverages this data to provide real-time insights, automate complex processes, enhance decision-making, and unlock new capabilities across industries. It powers self-driving cars, personalized medical

diagnostics, financial fraud detection, virtual customer support, and smart city infrastructures [3].

AI's ability to handle repetitive tasks, process vast datasets, and operate continuously without fatigue makes it a transformative force. It not only boosts efficiency but also opens new avenues in fields like healthcare, education, agriculture, and environmental protection, as shown in Fig (**1**). As we increasingly rely on digital systems, the role of AI continues to expand, making its understanding critical for both technical and non-technical audiences.

Fig. (1). AI in everyday life.

In addition, the chapter discusses the benefits AI brings to society, the challenges it poses, and the ethical questions it raises. It concludes with a glimpse into the future of AI, including emerging trends and the potential societal impact. Whether you are new to AI or seeking a structured overview, this chapter sets the stage for a deeper exploration of this exciting and fast-evolving field.

AI and Its Broad Influence

A diverse field that incorporates elements of computer science, mathematics, cognitive science, linguistics, neurology, and even philosophy, Artificial Intelligence is not a single technology. Its methods—such as supply chain optimization, energy grid management, weather forecasting, and digital marketing campaign customization—are ingrained in both the visible and unseen layers of contemporary infrastructure. Many people engage with AI on a regular basis without even noticing it because of how deeply integrated it is [4].

AI can be divided into two categories based on its capabilities: general AI, which is a more theoretical idea that refers to robots that could comprehend and learn any intellectual work that a person can, and narrow AI, also known as weak AI, which is made for specialized tasks like language translation or facial recognition. Although research on broad AI and human-level cognition is still ongoing, all deployed AI systems today fall within narrow AI [5].

CHAPTER 3

Strategic Integration of AI in Modern Cybersecurity Frameworks

LNC Prakash Koratamaddi[1], Goddumarri Suryanarayana[2], Lakshmi Hassan Nagaraja[3], Seema Nagaraj[4] and **Pundru Chandra Shaker Reddy[5,*]**

[1] *Department of Computer Science & Engineering-Data Science, CVR College of Engineering, Hyderabad, Telangna, India*

[2] *Symbiosis Institute of Technology, Hyderabad Campus, Symbiosis International University, Hyderabad, Telangana, India*

[3] *Department of CSE (AI&ML), CVR College of Engineering, Hyderabad, Telangana, India*

[4] *Department of MCA, Bangalore Institute of Technology, Bengaluru, Karnataka, India*

[5] *Amity School of Engineering and Technology Department of Computer Science and Engineering Amity University, Noida Uttar Pradesh, India*

Abstract: The rapid advancements in Artificial Intelligence (AI) have significantly transformed the landscape of cybersecurity, providing both new opportunities and challenges. This chapter explores the dynamic interplay between AI and cybersecurity, focusing on how AI-driven solutions enhance threat detection, incident response, and risk mitigation while also examining the emerging threats posed by AI-powered cyberattacks. AI has revolutionized cybersecurity by enabling intelligent automation, real-time threat analysis, and predictive modelling. Machine learning algorithms can detect anomalies, identify malware patterns, and adapt to evolving attack strategies, making cybersecurity defences more proactive and efficient. Deep learning techniques further enhance Intrusion Detection Systems (IDS), enabling faster and more accurate identification of potential security breaches. Additionally, AI-powered security frameworks strengthen authentication mechanisms, fraud detection, and vulnerability management, reducing human errors and response time. However, AI itself is a double-edged sword in cybersecurity. While it strengthens defences, cybercriminals increasingly leverage AI to develop sophisticated attack methods, including adversarial AI, deepfake-based social engineering, and automated hacking tools. The rise of AI-driven cyber threats demands an equally robust AI-driven defence mechanism, necessitating the development of explainable AI (XAI) for transparent decision-making and ethical AI governance to prevent misuse. This chapter provides a comprehensive analysis of AI's role in cybersecurity, discussing real-world applications, challenges, and future trends. It also highlights the ethical and regulatory considerations in deploying AI-based security solutions. By addressing these aspects, this chapter aims to provide a balanced perspective on harnessing AI's potential to build a resilient cyber-

* **Corresponding Author Pundru Chandra Shaker Reddy**: Amity School of Engineering and Technology Department of Computer Science and Engineering Amity University, Noida Uttar Pradesh, India; E-mail: chandu.pundru@gmail.com

Pundru Chandra Shaker Reddy, Yadala Sucharitha, & Thillaiarasu N (Eds.)

security framework while mitigating the risks associated with its adversarial applications.

Keywords: Artificial Intelligence, Cybersecurity, Explainable AI (XAI), Hacking, Intrusion Detection Systems (IDS), Machine learning, Social engineering, Vulnerability.

INTRODUCTION

In an increasingly interconnected digital world, cybersecurity has become a cornerstone of modern information infrastructure. As the volume, velocity, and variety of cyber threats continue to escalate, traditional approaches to securing digital assets are proving insufficient. The integration of Artificial Intelligence (AI) into cybersecurity offers a transformative approach to subdue these evolving threats. AI introduces a paradigm shift in how organizations detect, prevent, and respond to cyber incidents by leveraging data-driven insights, automation, and predictive capabilities [1]. The convergence of AI and cybersecurity represents a dual-use frontier. On one hand, AI empowers cybersecurity systems with enhanced pattern recognition, anomaly detection, and adaptive learning, helping security teams stay ahead of increasingly sophisticated threats [2]. On the other hand, adversaries are also adopting AI technologies to develop more complex and evasive attacks, such as adversarial machine learning and deepfake-based social engineering [3]. Traditionally, cybersecurity relied on signature-based systems and human expertise to identify threats and respond to breaches. These systems were effective against known threats but lacked the agility to detect zero-day exploits and novel malware variants. AI and machine Learning (ML) bridge this gap by enabling systems to learn from historical data, adapt to new threat signatures, and make intelligent decisions in real-time. One of the most impactful uses of AI in cybersecurity is in threat detection. Machine learning models, including supervised, unsupervised, and reinforcement learning, are employed to identify anomalous network behaviors, malware signatures, and phishing attempts [4]. Deep learning models further enhance intrusion detection systems by enabling faster, more accurate identification of malicious activity through pattern recognition across complex data [5]. AI also accelerates incident response by facilitating automation. Security Orchestration, Automation, and Response (SOAR) systems powered by AI can analyze logs, correlate threat intelligence, prioritize alerts, and initiate pre-defined mitigation protocols with minimal human intervention [6]. These capabilities drastically reduce response time and mitigate potential damage. In risk management and vulnerability assessment, AI tools scan vast codebases and network configurations to identify flaws, rank their severity, and recommend remediation strategies. Predictive analytics allow security teams to anticipate future threats and allocate resources efficiently [7]. Despite these

benefits, AI in cybersecurity presents challenges. Deep learning models are often black boxes, offering little interpretability regarding their decisions. This lack of transparency complicates accountability, especially when false positives or negatives occur [8]. Hence, the need for Explainable AI (XAI) becomes crucial in high-stakes security environments.

The threat landscape is further complicated by adversarial AI, where attackers manipulate input data to deceive AI systems. This includes evading malware detectors or fooling biometric systems with deepfakes [9]. The growing use of generative AI, such as large language models and synthetic media generators, poses a new set of risks that current cybersecurity models must adapt to. In this context, robust AI governance and ethical guidelines are essential. Policies must address data privacy, model robustness, transparency, and the misuse of AI technologies [10]. Regulatory bodies such as the EU have begun drafting AI regulations to mitigate these risks, but international collaboration remains necessary. Human expertise continues to be vital. While AI enhances capabilities, it cannot replace human intuition and ethical judgment. The most effective cybersecurity strategies involve human-AI collaboration, where each complements the other's strengths [11]. This chapter provides a comprehensive exploration of AI's applications, opportunities, and challenges in cybersecurity. It addresses emerging trends, adversarial risks, ethical concerns, and future research directions. By understanding both the potential and pitfalls of AI in cybersecurity, we can work towards building resilient, transparent, and ethical digital defense systems. Cybercrime losses reached a staggering $12.8 billion in 2023. Experts project these losses to hit $23.84 trillion by 2027. Organizations now face an average of 1,308 cyber-attacks weekly in early 2024 - a 28% increase from the previous quarter. AI-powered cybersecurity has emerged as a critical defense strategy, with 90% of organizations implementing these security solutions. The relationship between AI and cybersecurity cuts both ways. Organizations embrace these technologies faster than ever, yet 75% of cybersecurity experts report more frequent attacks. Bad actors using generative AI account for 85% of this increase. The situation looks more challenging since 59% of cybersecurity teams lack adequate staffing. Less than half of these teams feel confident they can detect and respond to threats effectively. This piece dives into artificial intelligence and cybersecurity approaches that deliver results in 2025. You'll discover proven AI-powered threat detection systems and automated security responses that work. We'll also help you calculate the ground ROI of your AI security investments.

LITERATURE SURVEY

The integration of Artificial Intelligence (AI) and Machine Learning (ML) into cybersecurity has significantly enhanced the detection, prevention, and mitigation

CHAPTER 4

Enhancing Cybersecurity in AI-Driven Environments: The Role of English Language Proficiency

Ranjit Kumar Elamadurthi[1], Goddumarri Suryanarayana[2] and **Pundru Chandra Shaker Reddy[3,*]**

[1] *Department of English, Vardhaman College of Engineering, Hyderabad, Telangana, India*

[2] *Symbiosis Institute of Technology, Hyderabad Campus, Symbiosis International University, Hyderabad, Telangana, India*

[3] *Amity School of Engineering and Technology, Department of CSE, Amity University, Noida, Uttar Pradesh, India*

Abstract: How firms detect, analyze, and respond to attacks has changed as cybersecurity systems incorporate AI. In the age of technology, human language abilities, especially English ability, are undervalued. In AI-driven cybersecurity scenarios, English proficiency affects threat interpretation, incident response, end-user interaction, and interface design. Linguistic clarity improves AI system communication, reducing miscommunication and speeding up multinational security operations. Standardized English is essential for understanding, expressing, and interpreting cybersecurity information in multilingual teams where AI relies on language inputs for correctness. Poor language abilities might mess up the procedure and miss subtle social engineering dangers. The report highlights the necessity for language ability to identify and address complex digital requirements by assessing current issues. Based on real-life case studies, NLP technology, and human-AI interaction models, the research recommends language training and English communication standards for cybersecurity procedures. The findings demonstrate the need for an interdisciplinary strategy that combines language and technological skills to improve cyber defense techniques in a changing digital world.

Keywords: Artificial Intelligence, Cyber-security, Communication, English Language Proficiency, Human-AI Interaction, Language-Aware Systems, Natural Language Processing (NLP), Security Protocols.

[*] **Corresponding Author Pundru Chandra Shaker Reddy:**, Amity School of Engineering and Technology, Department of CSE, Amity University, Noida, Uttar Pradesh, India; E-mail: chandu.pundru@gmail.com

INTRODUCTION

The advent and rapid proliferation of Artificial Intelligence (AI) technologies have ushered in a transformative era across various sectors, with cybersecurity emerging as one of the most profoundly affected domains. In the wake of escalating cyber threats and the ever-expanding digital landscape, organizations and governments alike are increasingly relying on AI-based solutions to safeguard their digital infrastructure. Unlike traditional cybersecurity tools that often operate reactively, AI-driven systems adopt a more dynamic, proactive, and adaptive posture, thereby fundamentally reshaping the paradigms of threat detection, incident response, and risk mitigation.

At the core of these systems lie cutting-edge computational paradigms such as Machine Learning (ML), Deep Learning (DL), and Natural Language Processing (NLP). These technologies empower cybersecurity systems with the ability to autonomously analyze large volumes of data, identify anomalies, detect patterns indicative of malicious activities, and even forecast potential threats before they materialize. For example, machine learning algorithms can continuously learn from historical attack data and behavioral logs to fine-tune their detection capabilities, while deep learning models, through convolutional or recurrent neural networks, can discern intricate, non-linear relationships within massive datasets that may elude human analysts [1]. Meanwhile, NLP enables the real-time parsing and interpretation of unstructured data from threat reports, darknet forums, phishing emails, and incident response documentation, thereby enriching situational awareness.

These advancements have not only enhanced the scalability and efficiency of cybersecurity operations but also significantly improved the resilience of digital ecosystems against an evolving and increasingly sophisticated landscape of cyberattacks. Modern threat actors—whether cybercriminal groups, state-sponsored adversaries, or hacktivists are employing complex Tactics, Techniques, and Procedures (TTPs), including polymorphic malware, zero-day exploits, AI-generated phishing content, ransomware-as-a-service (RaaS), and Advanced Persistent Threats (APTs). In such a context, traditional rule-based systems are often insufficient. AI-infused tools, by contrast, possess the capability to autonomously evolve and adapt in response to these dynamic challenges, making them indispensable in the contemporary cyber defense arsenal [2].

Despite the remarkable capabilities of these AI-enhanced cybersecurity frameworks, it is essential to recognize that their effectiveness is not solely contingent upon the sophistication of their algorithms, the speed of their processing units, or the granularity of their data sources. Rather, a critical yet

often overlooked factor lies in the human element, the cybersecurity professionals who develop, configure, maintain, and operate these complex systems. In other words, no matter how advanced an AI system may be, its operational utility, accuracy, and long-term relevance ultimately depend on the human decisions that guide its development and deployment.

This is where language, and specifically, English language proficiency, plays a crucial, though frequently underestimated, role. As cybersecurity becomes increasingly globalized, English has emerged as the *lingua franca* of the field. It serves as the principal medium for technical documentation, academic research, cybersecurity standards, cross-border communication, and the dissemination of real-time threat intelligence. From foundational texts like the MITRE ATT and CK framework and the NIST Cybersecurity Framework to vendor-specific documentation for tools such as TensorFlow, PyTorch, and Splunk, English dominates the informational and communicational infrastructure of cybersecurity [3].

Furthermore, collaboration among cybersecurity professionals rarely occurs within national silos. Cybersecurity operations now often span across geographies and time zones, with multinational teams working in tandem to respond to threats, share Indicators Of Compromise (IOCs), perform digital forensic analyses, and coordinate incident response strategies. These multinational collaborations depend heavily on clear and timely communication—much of which is conducted in English. In this context, a lack of proficiency in English can act as a barrier to effective communication, potentially leading to misinterpretations, delays in response, or incorrect configurations that can expose systems to risk [4].

The implications of this linguistic component are far-reaching. Cybersecurity practitioners who are not proficient in English may struggle to interpret critical security alerts, understand complex threat intelligence reports, or implement best practices outlined in international standards. Moreover, emerging cybersecurity professionals in non-English-speaking regions may face additional hurdles in accessing state-of-the-art AI tools and training resources, many of which are published exclusively in English. This linguistic gap can thus inadvertently widen the global cybersecurity skills gap, leaving certain organizations or regions more vulnerable to attacks.

In light of these observations, this work aims to explore the intricate and underexplored relationship between English language proficiency and cybersecurity efficacy in AI-driven environments. It argues that English language skills are not peripheral but foundational to the successful implementation and operation of AI-infused cybersecurity systems. By examining real-world case

CHAPTER 5

Leveraging Social Networks for Cyber Threat Intelligence: Attack Trends, Cybersecurity Threat Detection Challenges, AI-Based Solutions, and Potential Opportunities in X

Sri Rekha Uppuluri[1,*] and **Sasanko Sekhar Gantayat**[1]

[1] *School of Computer Science & AI, SR University, Warangal, Telangana, India*

Abstract: The increasing prevalence of cyber-attacks is a direct result of the ubiquitous nature of social media platforms like X (previously Twitter). This threat has prompted a plethora of research on ways to analyze X data for cyber-attack detection and prediction. This study primarily addresses the implementation of Artificial Intelligence (AI) approaches for anticipating future cyber risks on X. We argue that a semantic attention is more advantageous for this step of the method, even though character-level feature extraction approaches are copious. Our findings highlight the pervasiveness of social networks as a platform for the propagation of both valuable information and numerous security risks. Social media plays a significant role in spreading these cybercrime dangers; thus, addressing them must be a top priority. Our research shows that social media may be a powerful tool for cyber threat awareness and response. Data summarization levels, algorithm complexity, anticipation scope, kinds of cybersecurity threats, feature-extraction strategies, scalability over time, and performance measures are some of the important components that are generally under-evaluated in current studies. Examining current gaps and trends in this field, this chapter mainly seeks to discover AI algorithms employed for cyber threat detection on X. The study's findings on cyber threat dynamics and assault group methodology are useful for enhancing cybersecurity. It provides practical consequences for cybersecurity practitioners, law enforcement agencies, and lawmakers dedicated to protecting the digital environment, and highlights the crucial role of social networks in modern cyber-attack landscapes.

Key Terms: Anomaly detection, AI, Attack trends, Cybersecurity, NLP, Security &privacy, Social media, Twitter, Threat detection.

[*] **Corresponding Author Sri Rekha Uppuluri:**, School of Computer Science & AI, SR University, Warangal, Telangana, India; E-mail: 2403c50122@sru.edu.in

Pundru Chandra Shaker Reddy, Yadala Sucharitha, & Thillaiarasu N (Eds.)

INTRODUCTION

The introduction of AI has brought strong defenses as well as formidable threats, radically altering the cybersecurity scene. Despite AI's greatness in areas such as incident response, user authentication, and anomaly detection, bad actors are finding ways to leverage it to launch more complex assaults [1]. As a result of the intricate relationship between AI and human enemies, the threat landscape is always changing. A major threat to organizations is the rise of AI-powered attacks that may evade conventional defenses. A combination of sophisticated threat intelligence, flexible defenses, and a solid ethical foundation is necessary for effective countermeasures. Better threat detection, automated responses, and augmented human analysts are all possible outcomes of defensive AI deployment. However, cautious risk management is required due to issues including algorithmic bias, data privacy concerns, and the possibility of attacks driven by AI. Prioritizing regulatory compliance, industry standards, and collaboration is essential for enterprises to effectively harness the promise of AI in cybersecurity [2]. Investing in cybersecurity education and training is vital to establishing a knowledgeable workforce skilled in tackling evolving threats. The best way to reduce the dangers posed by AI and create a more robust digital environment is to close the gap between the two fields [3]. In recent years, social media platforms' cybersecurity has grown into a top priority. This is happening at the same time as the cybersecurity industry is seeing phenomenal growth, increasing by a factor of 35 in the last decade. The rising threat landscape is reflected in this increase in cybersecurity spending. Unfortunately, cybercrime has been on the rise alongside the expansion of the digital economy [4]. Data breaches put social media platforms and their users at risk, and the proliferation of internet and social media apps has given attackers additional possibilities to commit such crimes. The monetary loss due to cyberattacks is anticipated to triple from 2015 levels, reaching roughly USD 10.5 trillion per year by 2025, if the present trend continues [5]. Fig (**1**) shows the global investment in cybersecurity from 2017 to 2024.

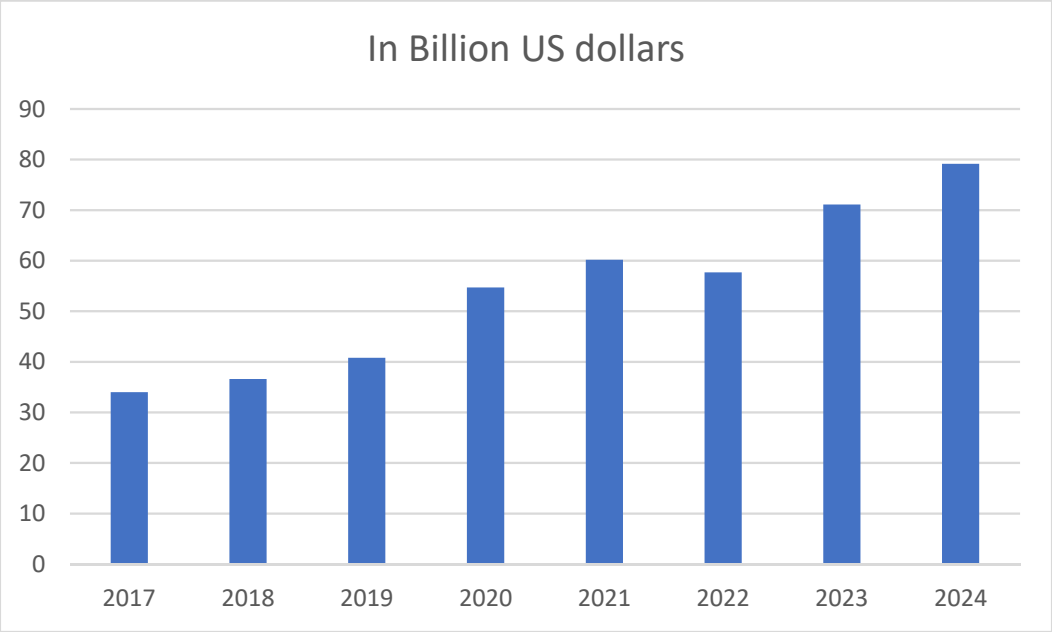


Fig. (1). Worldwide cybersecurity expenditure from 2017 to 2024.

Data analysis, pattern recognition, and automated processing are three areas where Artificial Intelligence (AI) technology excels, making it a formidable tool in the fight against cybersecurity threats [6]. Cybersecurity threat detection systems can improve their ability to spot unusual activity, uncover previously unseen dangers, and instantly adjust to changing assault patterns by utilizing technologies like deep learning and machine learning. Both the false alarm rate and the accuracy of threat detection are significantly reduced by this.

An authoritative resource for classifying and organizing newly discovered vulnerabilities according to the Common Vulnerability Exposures (CVE) standard, the National Vulnerability Database (NVD) helps businesses prioritize their efforts to fix these vulnerabilities. New research, however, suggests that the NVD might not get regular updates. Indeed, it is not uncommon for newly found vulnerabilities to be discussed on social media sites such as Twitter prior to their public disclosure on NVD, frequently without a CVE or prior to the appropriate announcement of a CVE [7]. By keeping tabs on and analyzing conversations happening within the cybersecurity community on Twitter, experts can get a head start in discovering exploitable flaws. This could help them find security holes before the NVD makes them public.

CHAPTER 6

Securing The Digital Frontier: A Comprehensive Guide to Modern Security Operations Centers (SOC)

Diivyaam Shah[1,*], **Kiran Dodiya**[1] and **Kapil Kumar**[1]

[1] *Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, India*

Abstract: An organization's cybersecurity infrastructure relies on a Security Operations Centre (SOC) in an age of fast cyber threat evolution. This chapter examines how SOCs protect against malware, ransomware, and advanced persistent threats as the first line of defense. A SOC monitors, analyzes, and responds to cybersecurity incidents, assesses alerts, and prioritizes threats by severity. A SOC's success depends on analysts and operations teams working together with integrated tools, processes, technologies, and policies to protect infrastructure. A modern Security Operations Centre (SOC) uses advanced threat intelligence, security automation, and orchestration technologies to detect and respond to threats. Security Operations Centers (SOCs) use various technologies and cybersecurity frameworks, including NIST, FedRAMP, FISMA, and MITRE ATT and CK, to improve security. These guidelines govern the SOC's plans and methods to prevent data breaches and assaults. SOC teams encounter obstacles from detection to investigation, containment, eradication, and recovery during cybersecurity incidents. It details the incident lifecycle, including SOC analysts' reaction processes and tools and techniques for speedy, effective, and complete action. This chapter examines the SOC operational lifecycle, highlights challenges in detection, investigation, and recovery, and introduces an AI-driven model to enhance efficiency, accuracy, and adaptability in threat response. It further emphasizes human–machine collaboration, skill development, and the integration of emerging technologies to build predictive and autonomous AI-augmented security environments.

Keywords: AI and ML, Analysts, Frameworks, Incident Response, SIEM, SOAR, SOC Lifecycle, SOC Team, SOC, Triage Specialist.

[*] **Corresponding Author Diivyaam Shah,**: Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, India; E-mail: shahdivyam2912@gmail.com

Pundru Chandra Shaker Reddy, Yadala Sucharitha, & Thillaiarasu N (Eds.)

INTRODUCTION

What is SOC?

The Security Operation Centre, also known as a Computer Emergency Response Team or Computer Security Incident Response Team, is dedicated to monitoring and analysing activity on networks, servers, endpoints, databases, applications, websites, and other systems that connect to your network, either locally or from a remote location. It is the first line of Defence that assesses different types of alerts and determines whether they're real or false positives. If implemented correctly, it can provide an overarching solution for detecting and mitigating an attack [1].

The role of SOC in Modern Cybersecurity

SOC does not just focus on developing a security strategy, designing a security architecture, or implementing protective measures. It is responsible for operational components of enterprise information security, improving the business's security posture through its products and services by introducing security as a shared responsibility [2]. A team that makes the most important strategic decisions at the time of an attack, when the attacker is attempting to breach a company's security to harm or steal their data, thereby ruining their reputation in the market and potentially leading to monetary loss.

Evolution of SOC in the Digital Age

From the 1970s to the early 2000s, traditional SOC, also known as a Network Operations Centre (NOC), primarily focused on incident detection and response, which included managing network devices and monitoring performance. In the early 2000s, after the introduction of Information Security Management Standards (ISMS) compliance, which was added to the objectives of the SOC. With the introduction of SIEM (Security Information and Event Management) platforms, which allowed analysts to collect logs centrally, automated alert generation based on predefined rules helped improve threat detection. As more sophisticated threats emerged and attackers became more advanced, SOC needed to change their strategies to incorporate advanced analysis, threat intelligence, and detection, along with active threat hunting, to detect and prevent advanced persistent threats in the late 2000s [3]. Presently, with the adoption of AI and ML, which has helped in faster detection and alert with minimal false positives. SOAR Security Orchestration, Automation, and Response tools help make an easy and simplified incident response workflow (Fig. **1**).

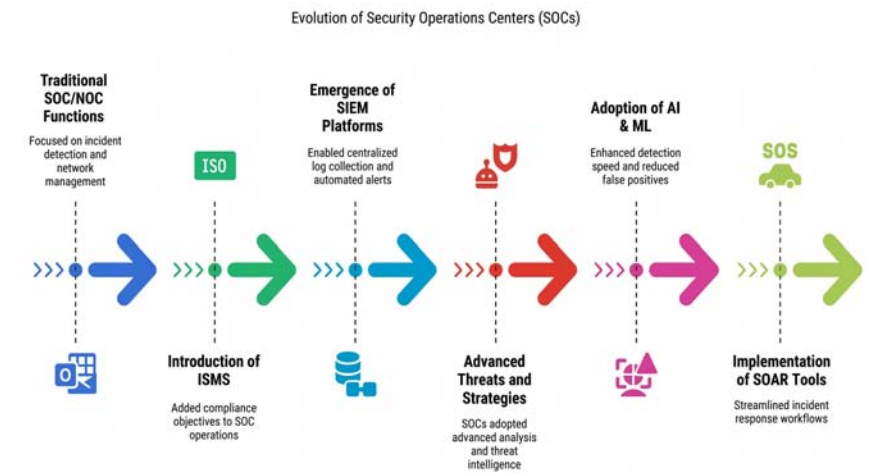


Fig. (1). Evolution of SOC in the digital era.

Literature Review

In the current world of evolving cyber threats, a Security Operations Centre (SOC) must also evolve rapidly to face such threats effectively. Traditionally, Security Operations Centers (SOCs) detected and responded to known threats only; however, in the modern approach, with the help of AI and other security tools, SOCs can actively identify and mitigate risks—the shift from reactive to proactive has helped improve SOC response times [4].

Regarding key components of SOCs, AI and ML have become core technologies in modern-era SOCs, enabling the investigation of incidents, triage of alerts, and recommendation of mitigations with high accuracy. ML algorithms are trained to detect APTs and reduce false positives, thereby achieving a higher percentage of accurate detections in the IT environment. Active defence strategies depend heavily on threat intelligence, which involves gathering, analysing, and disseminating information about potential threats. The integration of Extended Detection and Response (XDR), Zero Trust Architecture (ZTA), and Threat Intelligence Centres (TICs) collectively enhances the effectiveness of operations by enabling better prediction and mitigation of threats [5]. Automation helps streamline the incident response process and reduces human workload by speeding up the process of generating incident reports, providing background intelligence, and suggesting remediation steps. Orchestration tools integrate various security products, allowing for seamless communication and a coordinated response. Even after advancements, human expertise is highly required in SOCs as AI and humans work together to make ethical decisions, which helps solve problems such as AI bias [6].

CHAPTER 7

ML-based Endpoint Security: Advancing from Reactive Defense to Proactive Protection

S Nancy Lima Christy[1], C Santhosh Kumar[1], P Esaiarasi[2], N Gurusamy[3], N Shanmugapriya[4] and **K Madhan[5,*]**

[1] *Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India*

[2] *Department of Electronics and Communication Engineering, Mailam Engineering College, Mailam, Tamil Nadu, India*

[3] *Department of AI and DS, Sri Shanmugha College of Engineering and Technology, Sangakiri Salem, Tamil Nadu, India*

[4] *Department of Computer Science and Engineering, Dhanalakshmi Srinivasan University, Tamil Nadu, India*

[5] *Department of Information Technology, St. Joseph's College of Engineering, Chennai, Tamil Nadu, India*

Abstract: The rapidly changing cybersecurity environment makes enterprise system endpoints the main targets that cybercriminals use to gain access illegally. Web-based work and mobile devices, as well as IoT technologies, have substantially increased the potential attack space for endpoints. Modern cyber threats, along with ransomware-induced service attacks and fileless malware, and adversary artificial intelligence threats, diminish the effectiveness of traditional detection signatures at the endpoint. This chapter examines Artificial Intelligence that reinforces the defense at the endpoint to evolve towards predictive defense from conventional reactive controls. With machine learning partnered with natural language processing, along with behavioural analytics, AI enables real-time detection of threats, along with automation of incident response, while introducing security controls that adjust based on moving attack targets. It explains how AI-powered Endpoint Detection and Response technologies aid organizations in conducting anomaly detection coupled with active prevention of lateral movement activity, and realize threat response times that are prompt. The analysis displays how endpoint AI tools ought to be strategically added to enterprise threat intelligence systems to provide complete defense situational awareness and joint protection across all sections of the organization. The article discusses the ethical dimensions as well as regulatory positions while illustrating how generative AIs can evolve into systems that heal themselves while running autonomously to defend

[*] **Corresponding Author K. Madhan:** Department of Information Technology, St. Joseph's College of Engineering, Chennai, Tamil Nadu, India; E-mail: madhanckn@gmail.com

Pundru Chandra Shaker Reddy, Yadala Sucharitha, & Thillaiarasu N (Eds.)

endpoints. The chapter provides essential guidance to organizations that want to develop AI-based automated endpoint security capabilities within the context of contemporary cyber defense.

Keywords: Artificial Intelligence, Cybersecurity, Cyber Threats, Endpoint Detection, Endpoint security, Generative AIs, IoT technologies, Reactive Defense.

INTRODUCTION

The role of endpoint security in IT, as endpoint devices' security, became a key element of enterprise cybersecurity, as the traditional network barrier continues to disappear. From an endpoint protection aspect, things were relatively easy at first with a reliance on antivirus software to pick up and clean threats. But since endpoints were becoming more complicated and attackers were as well, endpoint security moved from chiefly being a process to keep the organization's desktop computers safe against malware and spyware [1]. This redirection embodies not only the evolving nature of cyber defense technologies but, more fundamentally, the shift from concentrating primarily upon known threats all the way to perceiving and responding to the unknown and evolving ones. This shift in defense strategies from basic baseline approaches to intelligent, adaptive, proactive models based on Artificial Intelligence (AI) demonstrates the mounting demand for intelligent, adaptive, and proactive models to safeguard enterprise endpoints [2].

This chapter aims to explore the transformative role of AI in redefining endpoint security. With the growing complexity of cyberattacks and the limitations of traditional reactive defense mechanisms, ML-based approaches offer intelligent, adaptive, and predictive capabilities that are essential for modern endpoint protection. The theme or focus of the chapter is on how the AI technologies– including Machine Learning (ML), Deep Learning (DL), and Reinforcement Learning (RL) enable proactive threat detection, automated response, and continuous security improvement.

Through the organization of the discussion into focused sections, this chapter provides both theoretical and practical insights. The primary objective of the chapter is as follows:

- To establish a comprehensive understanding of how AI augments endpoint security frameworks.
- To help cybersecurity professionals and researchers better defend against contemporary and future threats.

The chapter is organized as follows: Section 1 introduces the evolution of endpoint security, covering traditional endpoint protection mechanisms, the rise of API, and the shift from reactive to predictive security. Section 2 discusses the fundamentals of AI in cybersecurity, offering insights on the role of ML in threat classification, DL for malware detection, and RL in adaptive security models. Section 3 highlights ML-based endpoint detection and response-related concepts like behavioural analysis for endpoint anomaly detection, automated threat containment and remediation, and EDR integration in threat intelligence platforms. Section 4 concentrates on real-time threat detection using AI with in-depth analysis on stream processing for live data monitoring, predictive analysis for zero-day threats, and AI for phishing and social engineering detection. Section 5 is intended for the scope of AI in endpoint threat hunting, covering other concepts like data enrichment and correlation, identifying lateral movements in networks, and the use of graph analytics for threat tracing. Finally, Section 6 concludes the chapter by outlining the concepts discussed throughout, expressing the scope and fundamentals of AI in endpoint security.

The evolving cybersecurity landscape has made enterprise endpoints key targets for attackers, with web-based systems, mobile devices, and IoT expanding the threat surface. Traditional signature-based defenses are ineffective against modern threats like ransomware, fileless malware, and adversarial AI. Artificial Intelligence (AI) enhances endpoint protection through machine learning, natural language processing, and behavioral analytics, enabling real-time threat detection, automated response, and adaptive defenses. Real-world examples include **CrowdStrike Falcon**, which uses ML-based behavioral analytics to detect abnormal activities and prevent breaches, and **Microsoft Defender for Endpoint**, which applies deep learning and global threat intelligence to isolate compromised devices swiftly. The chapter concludes that AI-powered endpoint security, supported by ethical and regulatory compliance, predictive modeling, and skilled workforce development, is vital for building resilient, adaptive, and proactive cyber defenses.

EVOLUTION OF ENDPOINT SECURITY

Traditional Endpoint Protection Mechanisms

The early phase of digital security relied heavily on signature-based antivirus programs for endpoint protection. These tools worked by cross-referencing files and processes on a device against a database of known threat signatures. If a match was found, the system would quarantine or delete the suspected file. This worked well enough in an era where strains of malware were fewer and, in many cases, could be grouped together by their telltale attributes. More

CHAPTER 8

Sentiment Analysis with AI: Approaches, Datasets, Applications, Limitations, Challenges, and Future Directions

Nikita Gaur[1,*] and **Sridhar Chintala**[1]

[1] *School of Computer Science & AI, SR University, Warangal 506371, Telangana, India*

Abstract: One important area of NLP is Sentiment Analysis (SA), which involves classifying texts as either positive, negative, or neutral. Organizations must understand the sentiments underlying these ideas in order to make informed decisions, especially with the rise of online platforms where people can freely share their views and opinions. Improved customer happiness, stronger brand reputation, and more money can be achieved when businesses understand the feelings behind consumers' perceptions and attitudes towards their products and services. Political analysts can also use sentiment analysis to learn how the public feels about various parties, candidates, and policies. The financial sector can also make use of sentiment research to forecast stock prices and spot investment opportunities by analyzing news stories and social media posts. Including preprocessing approaches, feature extraction techniques, classification strategies, commonly utilized datasets, and investigational results, this chapter offers an overview of the newest breakthroughs in sentiment analysis. In addition, this chapter explores the difficulties of SA datasets, as well as their limitations and potential for further study. This chapter also offers insightful information about the current status of sentiment analysis, which is important for researchers and practitioners alike, because of the field's significance. Researchers and interested parties can use this document as a resource for up-to-date information on sentiment analysis and how the subject is evolving.

Keywords: AI, Deep learning, Machine learning, NLP, Opinion mining, Sentimental analysis, Social media, Text processing.

INTRODUCTION

The exponential evolution of the Internet over the past decade has occasioned an overwhelming volume of online comments; understanding the feelings of netizens

[*] **Corresponding Author: Nikita Gaur:** Research Scholar, School of Computer Science & AI, SR University, Warangal, Telangana, India; E-mail: 2403c50120@sru.edu.in

Pundru Chandra Shaker Reddy, Yadala Sucharitha, & Thillaiarasu N (Eds.)

through these comments is crucial to societal progress and stability. Emerging as a reply to this trend is SA expertise. Opinion mining, or SA, is a significant subfield in NLP that aims to automatically extract and assess viewpoints and sentiment from text. The advancement of AI cannot be achieved without SA [1]. We can find positive, neutral, and negative sentiments, which can be further subdivided into numerous subtypes. From a linguistic standpoint, studies involving sentiment analysis can make use of a wide range of natural languages, including English, Chinese, and many more. The only way for machines to respond intelligently is for them to study and comprehend human facial expressions, which will ultimately benefit humans. The growth of online social networks, e-commerce, banking, healthcare, and government all rely on SA [2]. Comments on websites are skyrocketing since most people's lives are now online. Public belief oversight and decision-making in many businesses can be aided by automatically scrutinizing tens of thousands of notes and recording the psychological thinking of contributors proficiently, rapidly, and cheaply.

An area of study within natural language processing known as sentiment analysis is concerned with the automatic detection and classification of feelings and opinions conveyed in written language. The proliferation of social-media platforms has greatly enhanced the accessibility of public thoughts and sentiments. As a result, sentiment analysis has become an indispensable tool for understanding public sentiment in many fields, including commerce, politics, and others. Preprocessing, feature extraction, and classification are three key processes in the SA process. Stop words, special characters, and digits are among the irrelevant information that are cleaned out of the raw text data through the preprocessing [3]. Tools like GloVe, word2vec, fastText, and Term Frequency-Inverse Document-Frequency (TF-IDF) are utilized to convert the text input into features during this step as well. The ML strategies, as well as DL models like RNN and LSTM, are used to categorize the processed text into feelings in the feature extraction stage.

Deep learning models like **LSTM** and **Transformers** enhance sentiment analysis by capturing contextual and semantic relationships in text. **LSTMs** retain long-term dependencies to interpret meaning across word sequences, while **Transformers** use attention mechanisms to analyze all word relationships simultaneously. This contextual understanding enables more accurate detection of sentiment, even in complex or ambiguous expressions.

To find out how the general population feels about a topic, Sentiment Analysis (SA) uses tools from the fields of NLP, Computational Linguistics (CL), and text analytics to extract opinions and other subjective information from source materials and then labels them as positive/negative or neutral. The intersection of

computers and human natural languages is the focus of NLP, a subfield of AI and linguistics [4]. By gleaning valuable insights from natively produced texts, NLP bridges the gap between machines and humans. Using several online data sources, SA aims to collect and analyze knowledge from personal data, reviews, and feedback. Sentence level, document level, and feature level are the three levels of SA. The goal here is to assign a favorable, negative, or neutral attitude to each opinion derived from a sentence, document, or aspect. Consequently, one can classify the methods according to their reliance on lexicons, machine learning, hybrid approaches, or, more recently, deep learning [5]. One method relies on algorithms trained on machine learning to identify and extract sentiment from data, while another uses a lexicon of sentiment terms, such as enhancement and negation, to count the number of positive and negative words in the data and determine the polarity of each phrase.

On the other hand, this approach relies on gleaning information from a statement that contains strongly held opinions. In the first stage of the deep learning-based approach, terms are learned by embedding them in the text corpus. The second stage uses these word embeddings to generate semantic composition interpretations of sentences using various deep learning approaches. Applying ML strategies greatly improves SA [6]. In this approach, a computer program is trained to carry out specific tasks, and it is said that the program has learned from its experience if and only if its measurable performance on these tasks improves over time. So, the data is the basis for the machine's decisions and forecasts. When training a model with labeled data is possible, a supervised learning strategy is utilized; otherwise, unsupervised learning is employed when the dependability of labeled data is questionable [7].

There are new opportunities to grasp people, groups, and society as a whole, thanks to the data collected from social media, which is currently the most dynamic signal base of human activity. Now more often referred to as “big social data,” the vast amounts of data produced by social media use exhibit computational properties such as large quantity, noise, and dynamic nature [8]. Due to its unique properties, it necessitates the application of appropriate computational methods for analysis. Using SA on social network data, we can see if there's any societal drift in people's opinions, perceptions, and expectations. Organizations are increasingly utilizing SA with ML approaches on social network data to get insight into user sentiment and opinion shared on these platforms, as well as to predict future organizational trends and identify areas for strategy change for improved efficiency and effectiveness [9]. From keeping tabs on how people feel about a certain business to seeing how people feel about certain political or social issues to seeing trends and patterns in user opinions—which can help with decision-making—it has many potential uses.

CHAPTER 9

Leveraging Artificial Intelligence and Blockchain: Feasibility of Integration, Research Issues, Applications, Challenges, and Future Directions

Rayapati Venkata Sudhakar[1], Karibasappa Chatrapathi[2], Sridhar N Koka[3], Vijay Bhanudas Gujar[4], Yadala Sucharitha[5,*] and **Mudarakola Lakshmi Prasad[6]**

[1] *Department of Computer Science and Engineering, Geethanjali College of Engineering and Technology, Hyderabad, Telangana, India*

[2] *School of Computing & Information Technology, REVA University, Bangalore, Karnataka, India*

[3] *Faculty of Business Administration, Panyapiwat Institute of Management, Pak Kret, Nonthaburi, Thailand*

[4] *Computer Science and Engineering Department, Arvind Gavali College of Engineering, Satara, Maharashtra, India*

[5] *Sharda School of Computing Science and Engineering, Department of CSE, Sharda University, Greater Noida, Uttar Pradesh, India*

[6] *Computer Science and Engineering, Institute of Aeronautical Engineering, Dundigal, Telangana, India*

Abstract: Blockchain is a decentralised ledger technology that has several applications in the financial sector, IoT, big data, cloud computing, and edge computing because of its distributed point-to-point architecture, which provides a secure and provable method for validating transactions. However, AI is progressively fostering the intelligent development of numerous sectors. Converging blockchain and AI technology has obvious benefits, since they are two of the most promising technologies in use today. Both blockchain and AI can work together to make AI smarter; AI can make blockchain more trustworthy and autonomous, and AI can make blockchain smarter. The integration of blockchain technology with AI is examined in this article from a more holistic and multi-faceted perspective. Before delving into an analysis of the potential for a blockchain-AI hybrid, we provide some context for both systems by outlining AI's history and the idea, traits, and core technology of blockchain. Our next step is to provide a synopsis of the relevant domestic and international research on blockchain and AI convergence. Following that, we will go over a few connected use cases regarding the merging of the two technologies. Additionally, the assessment covers the current state of these systems, the difficulties they continue to encounter as a

[*] **Corresponding Author Yadala Sucharitha**: Sharda School of Computing Science and Engineering, Department of CSE, Sharda University, Greater Noida, Uttar Pradesh, India; suchi.yadala@gmail.com

Pundru Chandra Shaker Reddy, Yadala Sucharitha, & Thillaiarasu N (Eds.)

result of the AI and blockchain algorithms that power them, as well as the potential areas for future research. An overview of the study area from many angles is provided by the analysis's results.

Keywords: Applications, Artificial intelligence, Blockchain, Machine Learning, Security.

INTRODUCTION

The indispensable role that blockchain and AI play in scientific innovation and industrial transformation has led to them attracting increased attention as cutting-edge technologies currently [1]. In 1956, the Dartmouth Society came up with the idea of AI technology. An integral part of computer science, AI technology seeks to model, augment, and improve upon human intellect through the study and application of technical sciences. The exponential growth of data and the remarkable advances in Machine Learning (ML), particularly Deep Learning (DL), have ushered in a new era of explosive growth in artificial intelligence in recent years. Industries like education, retail, transportation, security, and finance stand to gain greatly from artificial intelligence's prowess in analysis, prediction, judgment, and decision-making [2]. The concept of blockchain technology did not emerge until 2008, when Satoshi Nakamoto introduced Bitcoin. A distributed ledger is the basic idea behind the blockchain [3]. Without the need for an intermediary, it is able to use a decentralized consensus process in a multi-entity setting. In addition to facilitating the creation and verification of transactions in a decentralized, untrusted system, blockchain technology allows for the cost-effective development of trust [4]. For this reason alone, blockchain technology has attracted a growing number of academics.

In Fig. (**1**), we can see an overview of the AI terminology. Any system that makes decisions by consulting a database is said to have artificial intelligence (AI). It is possible to teach computers to make decisions using massive amounts of data through a branch of artificial intelligence known as machine learning (ML). An area of machine learning known as a neural network draws inspiration from the way the human brain works [5]. Inside, you'll find the building blocks of an input, multiple hidden, and output layers. The foundation of deep learning is a network of interconnected brain units called a “neural network,” which employs these layers to refine feature extraction over time.

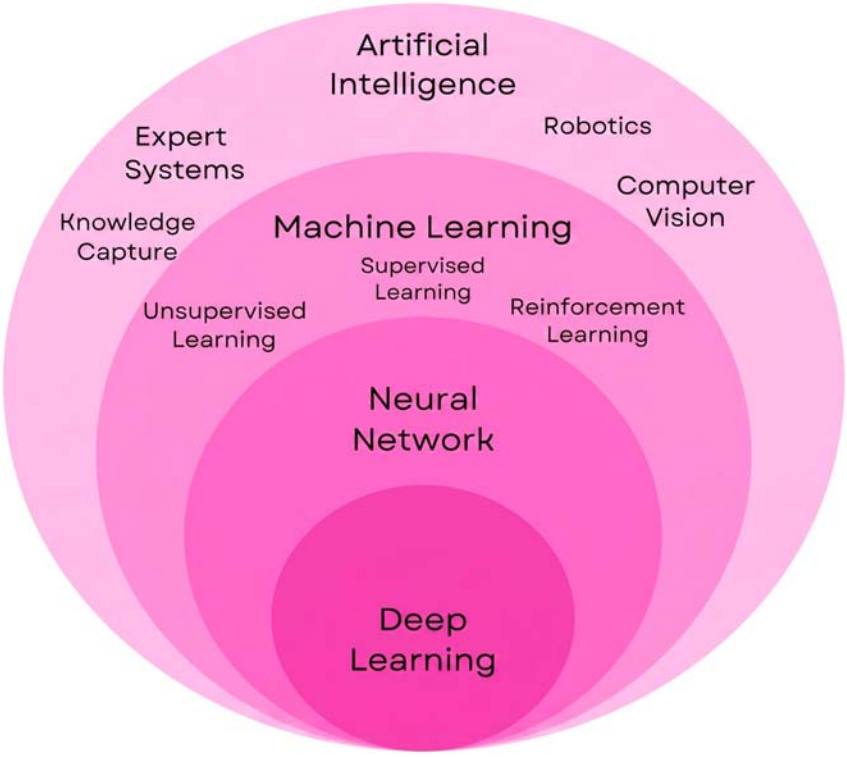


Fig. (1). Structure of the AI.

Recent developments in blockchain-related systems have opened up new possibilities for decentralized environments, even if AI has been flourishing across many industries, particularly healthcare, for the past few years. The significance of up-to-the-minute data became clear as the COVID-19 pandemic progressed [6]. Faster and faster mobile healthcare is replacing the antiquated patient-hospital-based system. This is particularly true in light of new innovations like the Internet of Medical Things (IoMT), which allow for the remote tracking and monitoring of a wide range of health conditions through smart devices [7]. Although this simplifies a lot of work and makes things more reliable, it generates and transmits a lot of sensitive medical data, which must be protected. In Fig. (**2**), we can see how AI and blockchain work together. In this setup, data is gathered by sensors and smart devices, then delivered to smart applications that analyze and predict using blockchain platforms and machine learning models [8].

CHAPTER 10

AI-Driven Cybersecurity Framework for SRI Funds: Ensuring Ethical Compliance and Risk Mitigation

Ambati Suvarna[1,*] and **Kafila**[1]

[1] *School of Business, SR University, Warangal, Telangana, India*

Abstract: Funds under the purview of socially responsible investment strive to promote ethical practices in investment and financing methods, making cybersecurity an important prerequisite for building investor confidence and ensuring compliance with laws and regulations. This paper presents an AI-based cybersecurity framework designed to advance the security, compliance, and risk management of SRI funds. It also considers risk management methods, including AI predictive analytics, mitigation of insider threats through AI, and transparency through blockchain affiliation. One main impediment for SRI funds is ensuring proper ethical compliance, warranting automation of regulatory frameworks using AI and comparative analysis of various global cybersecurity regulations on SRI investments. By way of case studies, the paper explores the transformational role of AI in cybersecurity. BlackRock's real-world case of internal AI deployment for fraud detection serves as an example of reducing financial threats and improving investor confidence using cyber-secured systems powered by AI. Along the same lines, HSBC's implementation of automation under AI ensures compliance with ESG at a pace that demonstrates the efficiency of AI in sticking to the regulations. AI improves monitoring for cybersecurity, automates compliance with ESG regulations, and links to blockchain for making secure transactions. Threats to all of these developments abound, such as AI-powered cybercrime, shifts across borders in regulation, and vagaries in ethical AI. The end of the paper provides recommendations for adopting AI strategies for a more resilient, compliant, and safe SRI investment ecosystem for fund managers.

Keywords: AI-driven cybersecurity, AI-Based Fraud Detection, Blockchain Transparency, Cyber Risk Management, ESG Regulatory Compliance, Ethical AI in Finance, SRI Fund Security, Sustainable Investment Technology.

[*] **Corresponding Author Ambati Suvarna:**, School of Business, SR University, Warangal, Telangana, India; E-mail: ambatisuv786@gmail.com

Pundru Chandra Shaker Reddy, Yadala Sucharitha, & Thillaiarasu N (Eds.)

INTRODUCTION

With the accelerated digitization of financial services, including SRI, data security increasingly emerged as an issue of ethical compliance and risk mitigation. Ethical SRI funds, which consider the environmental, social, and governance framework in making their investment decisions, should have a mechanism to ascertain ethical alignment amidst a cyber-attacking environment. In line with this, AI-based cybersecurity systems have increasingly assisted. Such systems intervene with real-time threat determinations, anomaly detections, and enable compliance automation [1, 2].

The environment of this paper is a compelling combination of the need for strengthening cybersecurity systems in an SRI environment where financial integrity and social responsibility coexist. The approach to designing, analyzing, and evaluating a cybersecurity framework that an AI would use to make the environment more resilient toward threats, ensure adherence to international ESG regulations, and abide by ethical AI must [3, 4]. AI brings with it groundbreaking tools for predictive analysis and fraud detection, also bringing with it new types of risks, such as adversarial attacks and algorithmic bias, that require being treated by a multidisciplinary approach [5].

This paper emphasizes a comprehensive theme: integrating ethical, regulatory, and technological safeguards into AI-powered security systems tailored for SRI funds. In doing so, it supports the broader vision of using responsible innovation to protect investor trust and regulatory adherence in sustainable finance [6].

OVERVIEW OF SRI FUNDS

Recently, there has been a great deal of attention on Socially Responsible Investment (SRI) funds, and their growth and impact have been thoroughly studied in various markets. SRI has evolved from a niche and primarily religious exclusionary practice into a mainstream risk analysis strategy for institutional and retail investors, according to [7]. However, although some researchers claim that SRI funds appear to be more promising in some areas, their actual impact on corporate behavior has also been subject to skepticism. A recent study indicated that SRI funds target firms promoting better environmental and social conduct, but do not change the behavior of firms or actively engage in shareholder proposals to effect change [8]. On the other hand, many remaining challenges are recognized by the lack of a global common taxonomy on sustainable activities, legislative clarity, and quality data for cross-industry and cross-regional comparison [7].

IMPORTANCE OF CYBERSECURITY IN FINANCIAL MARKETS

Cybersecurity is a focal discussion in the increasingly emerging financial institutions, as their common concern nowadays is frequent and sophisticated cyberattacks [9]. The rapidly developing financial technologies (FinTech) have brought tremendous changes to the financial landscape: advanced convenience and speed in service delivery, but unfortunately, exposing the sector to even more complicated issues in cybersecurity threats. Cybersecurity threats include traditional attacks from phishing to malware and sophisticated attacks like supply chain attacks, AI-driven cyber threats, and ransomware [10]. Interestingly, while cybersecurity measures are essential, there is also a concept that complements the existing paradigm of cybersecurity, called cyber-resilience. Cyber-resilience will thus enable very complex organizations to prepare for adverse events such as cyber-risk-induced external shocks, which they are supposed to withstand, recover from, and adapt to. In a nutshell, importance cannot be overestimated when it comes to financial markets and cybersecurity. It is also about the protection of private customer information, the integrity of transactions, and trust maintained in the digital financial environment [11]. A holistic approach to cybersecurity will enhance this for the financial institutions in terms of user awareness, technical measures, preparedness for incidents, and regulatory compliance to maneuver through confident resilience in a digital landscape [12]. As evolving technology transforms the relationships within the financial industry, a proactive and adaptive cybersecurity strategy in advance will guarantee the viability of the financial ecosystem against growing and more complex cyber threats [10].

ROLE OF AI IN ENHANCING SECURITY AND COMPLIANCE

AI serves as a fundamental lever to enhance security and compliance systems across multiple sectors with the additional benefits of risk management, threat detection, and regulatory compliance. In the case of hospital-integrated risk management, AI contributes to patient safety by facilitating early detection of critical conditions and enhancing clinical risk management [13]. In the sphere of cybersecurity, AI systems are doing far better than their human counterparts in dealing with increasing volumes of data, being able to detect anomalies and identify patterns that would have most likely gone unnoticed by conventional security systems, and thus improve the prediction and trend analyses to plug possible loopholes [2]. Ironically, despite the introduction of AI as a powerful tool in security and compliance, newer challenges have arisen. The introduction of AI brings with it adversarial threats, concerns regarding data privacy, and a clear view of the transparency of AI in its decision-making processes in the area of cybersecurity [2]. In healthcare, the use of AI likewise raises issues bordering on data privacy and security, as well as the need for sound cybersecurity measures

CHAPTER 11

Security in Smart Cities: Applications, Advances, Practices, Research Challenges, and Future Trends

M Indrasenareddy[1,*], K Venkatesh[2], K Chatrapathy[3], D Chitra[4], S Yuvalatha[5] and **M Lakshmi Prasad[6]**

[1] *Computer Science and Engineering, BVRIT HYDERABAD College, of Engineering for Women, Hyderabad, Telangana, India*

[2] *Department of Engineering in Internetworking, Dalhousie University, Halifax, Nova Scotia, Canada*

[3] *School of Computing & Information Technology, REVA University Bangalore, Karnataka, India*

[4] *Department of MBA, Panimalar Engineering College, Chennai, Tamil Nadu, India*

[5] *Department of Computer Science and Business Systems, Bannari Amman Institute of Technology, Erode, Tamil Nadu, India*

[6] *Computer Science and Engineering, Institute of Aeronautical Engineering, Hyderabad, Telangana, India*

Abstract: The concept of "smart cities" is gaining traction around the world, with several governments allocating substantial funds to this cause. The concept of smart cities has developed gradually over the years, moving from prior efforts on the smart city to more recent iterations such as eco-city, sustainable city, linked city, omnipresent city, and green city. The advent of lightning-fast 5G wireless connectivity, lightning-fast GPU multi-core servers, big data, cloud computing, AI, and data analytics are all hallmarks of the modern era. The creation and implementation of "smart cities" have been aided by numerous emerging technologies. To better comprehend what we meant when we said "securing smart cities," the authors of this paper lay out a framework for doing just that. They go over the pros and cons of using current security measures to protect a smart city, including authentication, access control, encryption, and firewalls. In particular, we discuss the potential harmful assaults on a smart city and the repercussions of such attacks, as well as the security of data, the internet, water supply, electricity supply, the city brain, and other vital city services. Lastly, they go over some smartcity security best practices. Additionally, this chapter delves into the idea of smart cities and how the IoT and ML may be utilized to create a data-driven smart environment. By maximizing the use of data and technology, "smart cities" raise living standards for city dwellers and make municipal services more efficient. In addition to outlining the many uses of smart cities, this chapter delves into the difficulties of integrating IoT and ML into cityscapes.

[*] **Corresponding Author M Indrasenareddy:** Department of Computer Science and Engineering, BVRIT Hyderabad College of Engineering for Women, Hyderabad, Telangana, India;
Email: indrasenareddy.m@bvrithyderabad.edu.in

Pundru Chandra Shaker Reddy, Yadala Sucharitha, & Thillaiarasu N (Eds.)

Keywords: IoT, Machine Learning, Smart-cities, Security, 5G.

INTRODUCTION

To integrate cutting-edge software and hardware based on information and communication technology (ICT) into city planning, the concept of a "smart city" was initially proposed in 1990. A smart city is one that makes use of information and communiqué technologies to improve the quality of life for its residents, boost the economy, make it easier to manage transportation and traffic, promote environmental sustainability, and make it easier for people to communicate with government officials. Planners are increasingly drawn to the smart city concept as a means to address the growing urban population and new developments in urban planning and information and communication technology [1]. This approach prioritizes the well-being of city dwellers by addressing various technological, social, cultural, environmental, energy, and information needs. Research has pointed to smart mobility as an aspect of the smart city concept (Apostol). The goal of smart city planning is to employ cutting-edge technology and processes to address pressing urban issues such as traffic jams, energy networks with high carbon emissions, inadequate infrastructure, and a lack of public safety and sound policy. Some examples of cities that have embraced AI and robots to create smart applications are Ottawa, Moscow, Dubai, London, New York, and Hong Kong [2]. Keep in mind that these technologies aren't without their risks, and those risks could compromise a smart city's ability to function.

The intricacy of the systems required for smart city development makes smart city systems vulnerable in terms of their functionality. Such susceptibility may arise as a result of external risks, strategy risks, or operational risks. The authors of [3] list the potential dangers that smart cities face, including approval issues, financial concerns, technological challenges, difficulties in forming partnerships, and problems with managing resources. The privacy and security of the smart city technologies are potential weak points. It may be easier to identify risks in smart city systems on an individual level, which means that risk management strategies can be better put into place to lessen their impact [4]. For instance, the hazards associated with energy systems are brought to light by. They talk about the smart city waste management system's hazards and difficulties. When evaluating risks associated with smart city planning and management, however, research should take the big picture into account. If smart city projects are to overcome obstacles in areas such as technology, privacy and security, politics, the environment, management, and user trust and acceptance, it is crucial to evaluate all of these risks simultaneously [5]. Various parts of a smart city's design and operation may have potential dangers that a risk assessment like this one can reveal.

A lot of processing power is needed to handle this mountain of data used to integrate different AI and ML algorithms. For instance, in the last several years, machine learning and artificial intelligence have been employed by practically all medical and clinical science institutes [6]. When it comes to smart health, radiology is a really effective field that uses AI and ML to great advantage. On a yearly basis, over two billion medical exams and scans, such as chest X-rays, are conducted around the world. Many different types of medical images make use of Deep Neural Networks (DNN), a well-known deep learning algorithm [7]. Management of water or electricity resources, verification, and payment for intelligent card services are only a few examples of the many important applications that have recently adopted a data-centric architecture. Smart mobility has the potential to increase traffic efficiency while decreasing CO_2 emissions. Information gathering, data networking, and pervasiveness are crucial to the smart city applications and their utility [8]. Fig. (**1**) shows how smart cities are good for people and the environment.

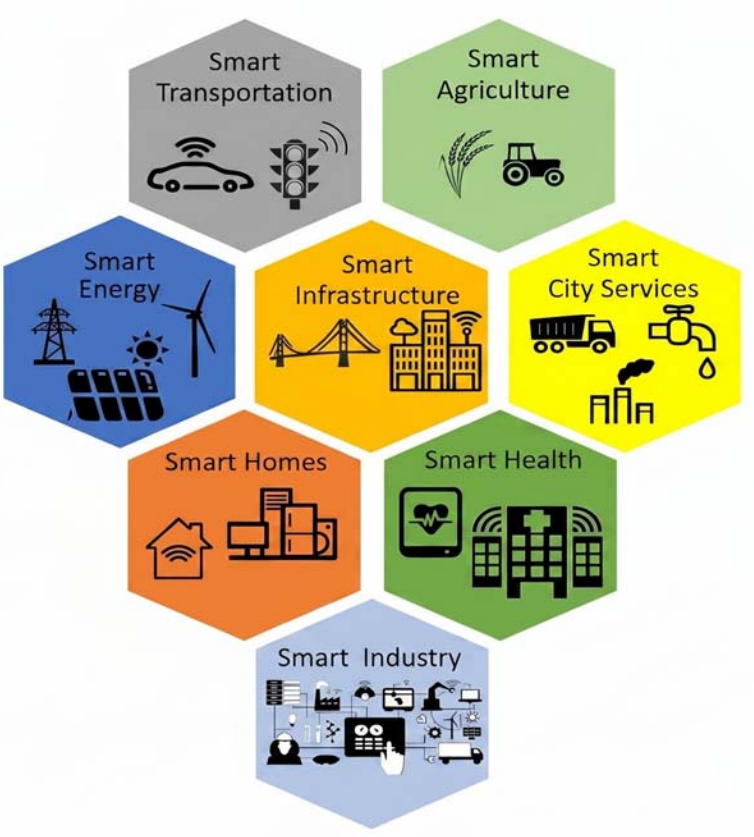


Fig. (1). Smart cities components.

CHAPTER 12

AI for Next Generation: Emerging Trends and Future Directions

Ramesh Babu Pittala[1,*], Niteesha Sharma[1], Thinagaran Perumal[2], Medikonda Asha Kiran[1], Manyam Thaile[1] and **Peddada Nagamani[1]**

[1] *Department of Information Technology, School of Engineering, Anurag University, Hyderabad, Telangana, India*

[2] *Department of Computer Science, University Putra Malaysia, Serdang, Selangor, Malaysia*

Abstract: Artificial Intelligence (AI) is revolutionizing modern technology, reshaping industries, and redefining cybersecurity. This chapter comprehensively introduces AI, offering insights into its evolution, core principles, and diverse applications. This chapter introduces AI briefly, delving into its history, key concepts, methodologies, and various applications. It delves into major AI paradigms like machine learning, deep learning, and natural language processing, which are revolutionizing data-driven decision-making. AI in cybersecurity is proving to be a game-changer, where it is being leveraged for threat detection, response automation, and enhanced enterprise security infrastructure. This chapter reviews how AI-driven prevention enhances threat intelligence by detecting anomalies, predicting cyberattacks, and mitigating real-time risks. It also talks about ethical issues of AI implementation, like bias, interpretability, and accountability, which are essential for responsible AI deployment in security ops. Setting the stage for a deeper dive into AI-driven cybersecurity frameworks in later chapters, this chapter creates a promising basis for understanding AI. It blows the whistle on AI-powered threat intelligence, automated incident response, and the future of AI in enterprise security.

Keywords: AI Applications, AI Ethics, AI In Cyber Security, AI Techniques, AI Thinking, Automated Cyber Security, Cyber Security, Deep Learning, Enterprise Security, Human Language, Machine Learning, Narrow AI, Neural Networks, Perception, Threat Detection.

[*] **Corresponding Author Ramesh Babu Pittala**: Department of Information Technology, School of Engineering, Anurag University, Hyderabad, Telangana, India; E-mail: prameshbabu526@gmail.com

Pundru Chandra Shaker Reddy, Yadala Sucharitha, & Thillaiarasu N (Eds.)

INTRODUCTION

What Exactly is Artificial Intelligence (AI)?

Artificial Intelligence (AI) is a branch of computer science that focuses on building intelligent systems capable of performing tasks that typically require human intelligence. These tasks include learning, reasoning, perception, language understanding, and decision-making [1]. AI systems can analyze data, identify patterns, adapt over time, and autonomously respond to complex environments. AI aims to replicate and enhance human-like cognitive abilities, enabling machines to operate independently and efficiently in various domains such as healthcare, finance, cybersecurity, and autonomous systems.

AI will impact **healthcare** through faster diagnosis, personalized treatment, and predictive analytics for disease prevention. In **education**, it will enable adaptive learning, automated assessments, and personalized student support. In **finance**, AI will enhance fraud detection, risk management, and automated decision-making, improving efficiency and security across services.

The four components constituting AI technology are as follows and are depicted in Fig. (**1**), which include:

i. Learning
ii. Reasoning
iii. Perception skills
iv. Language understanding

Learning: The Core of Machine Intelligence

In AI, a machine is considered to learn if it enhances its performance in a defined task due to experience or data processing. AI systems outperform software applications because they build upon performance-enhancing algorithms that operate automatically after analyzing vast amounts of data, unlike earlier programmed software systems that required extensive manual coding. The primary reason behind this is the aspect of learning referred to as Machine Learning (ML), which acts as a sub-branch under the umbrella of Artificial Intelligence (AI). ML algorithms scan data and identify trends among the vast amounts of repetitive information stored in databases [2]. The trained model makes predictions or decisions concerning unprocessed data sets from the processed data. The spam filter application learns from past messages by extracting features from messages sent to the user to determine which messages should be sent to the user in the future. Different aspects of machine learning can be classified into three branches.

In **supervised learning**, the model trains itself on input-output data, also called a training set, where the input consists of predefined outputs, known as labels. By providing the system with appropriate data, the predictive functions of the algorithms are formed. Rather than having a specific **classification model**, the system analyzes patterns in the data. This approach is mainly used for item groupings and anomaly detection. Agents learn to make **decisions** based on interactions with the environment and receive performance feedback through rewards and punishments. This kind of learning is mainly applied in robotics and game-playing AI [3].

Reasoning: Abilities AI Thinks With

AI systems achieve reasoning through the ability to process facts and determine conclusions and decisions that are logically or evidentially supported. Artificial intelligence accomplishes operational tasks logically based on artificial principles by reasoning based on its operational premises and processes. It concludes from its premises or conditions during its logical AI preconditions. AI systems employ optimization methods that determine the best decisions by setting achievable targets, such as minimizing costs or time for the reasoning stage. All the known information AI systems have access to allows for the formulation of new conclusions and making future predictions [4]. With patient data, an AI system can accurately estimate the probability of a patient developing a particular disease. AI perceives system learning patterns through traffic monitoring, which uncovers vertex activities that are quadratically abnormal with possible malicious intent, showing distinctions without explicit attack definitions. Perception is the ability of artificial intelligence to receive information from the environment and understand that it receives information from the outside world [5]. Machines need the ability to both obtain and comprehend information through using the senses as perception. Unlike humans, who rely on the five senses, AI systems acquire an understanding of the environment by processing data from sensors, cameras, microphones, and devices that provide feedback.

Perception: Computer Vision, A branch of AI

The perception of images and videos as objects is called computer vision, a branch of AI functionality. AI can now perform advanced face and motion tracking, scene analysis, and object classification through sophisticated neural networks and algorithms. These capabilities are now integrated into machines, enabling them to 'see' and 'interpret' data for various applications, such as security, facial recognition, and autonomous vehicle navigation. The AI systems perceive their surroundings with sound monitors that enable speech recognition and other devices that offer tactile feedback [6]. Autonomous vehicles use AI alongside

SUBJECT INDEX

W

X

Y

Z

P. Chandra Shaker Reddy

Dr. P. Chandra Shaker Reddy is a Professor in the Department of Computer Science and Engineering at Amity University, Noida, Uttar Pradesh, India. He has over 18 years of teaching and research experience in artificial intelligence, cybersecurity, machine learning, and data-driven intelligent systems. Dr. Reddy has published approximately 120 research articles in reputed international journals and conferences. His scholarly contributions have received over 2,300 citations, with an h-index of 32 as indexed by Scopus. He has also authored book chapters, patents, and has supervised postgraduate and doctoral research.

Yadala Sucharitha

Dr. Yadala Sucharitha is an Associate Professor in the Department of Computer Science and Engineering at Sharda University, Greater Noida, Uttar Pradesh, India. He has over 16 years of teaching and research experience in computer science, with research interests spanning artificial intelligence, data analytics, and cybersecurity. Dr. Sucharitha has published around 40 research papers in reputed national and international journals and conferences. His scholarly work has received more than 600 citations, with an h-index of 11 as indexed by Scopus. He is actively involved in academic mentoring and research supervision.

Thillaiarasu Nadesan

Dr. Thillaiarasu Nadesan is an Associate Professor in the School of CS & IT at REVA University, Bengaluru, Karnataka, India. He is an experienced academician and researcher with expertise in cybersecurity, artificial intelligence, and advanced computing technologies. His research interests include intelligent security systems, cyber threat analysis, and AI-driven frameworks for enterprise and emerging digital environments. Dr. Nadesan has contributed to scholarly research through journal and conference publications and is actively involved in teaching, research guidance, and academic development activities, with a strong focus on innovation and future-ready security solutions.