

Midocean University

College of Informatics

Department of Artificial Intelligence



CYBERSECURITY AND THREAT DETECTION

Prepared by:

Sultan Khalaf Alotaibi (222000226)

Supervised by:

Dr.Mohammed Anbar

First semester 2025

TABLE OF CONTENTS

ABSTRACT	1
CHAPTER 1	3
1.0 INTRODUCTION.....	3
1.1 BACKGROUND.....	4
1.2 PROBLEM STATEMENT	6
1.3 RESEARCH OBJECTIVES	8
1.4 RESEARCH SCOPE	8
CHAPTER 2	10
2.0 LITERATURE REVIEW.....	10
2.1 CRITICAL ANALYSIS.....	12
2.2 CONNECTIONS AND CONFLICTS.....	12
CHAPTER 3	13
3.0 RESEARCH METHODOLOGY	13
3.1 GANTT CHART.....	17
REFERENCES	18

ABSTRACT

Rising complexity and frequency of cyber threats have made conventional cybersecurity systems useless in identifying and minimizing sophisticated attacks including zero-day exploits, inside threats, and advanced phishing techniques. Particularly in Internet of Things (IoT) and cloud-based settings, these risks represent a major challenge to digital infrastructures. Limited in flexibility and scalability, traditional rule-based and signature-based systems frequently yield high false-positive rates and lack the sensitivity required for changing threat environments.

The aim of this study is to better real-time threat detection, behavioural analytics, and automatic incident response by including artificial intelligence (AI), machine learning (ML), and deep learning techniques into cybersecurity systems. We investigate how Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Natural Language Processing (NLP) can be used to tackle current cybersecurity issues. It stresses the ethical, openness, and adversarial resiliency concerns related with AI deployment, including training data set inherent prejudices and computational overhead.

Using a mixed-methods approach, the research covers four phases: a thorough literature review, qualitative data gathering through case studies and expert interviews, structured surveys, and the creation and validation of an adaptive AI-driven cybersecurity framework. The suggested system seeks to improve explainability, guarantee smooth integration with current systems, maximize computational efficiency, and foster ethical transparency.

Expert reviews and pilot testing results verify the possibility of the framework to enhance real-time threat response, adversarial defence, and operational scalability in resource-constrained environments. By tackling existing constraints and providing a practically

implementable, ethically grounded, and robust AI-based solution, this study adds much to the knowledge of cybersecurity.

Keywords: Cybersecurity, Threat Detection, Artificial Intelligence, Machine Learning, Deep Learning, Convolutional Neural Networks, Recurrent Neural Networks, Natural Language Processing, Insider Threats, IoT Security, Ethical AI, Adversarial Robustness, Real-time Threat Response, Computational Efficiency, Explainability, Framework Development.

CHAPTER 1

1.0 INTRODUCTION

Cybersecurity threats have progressed speedily and become more advanced and difficult to spot and stop properly in the modern digital environment than can be solved by traditional means. Mostly depending on rule-based systems and signature-based threat detection tools, traditional cybersecurity methods falter quite a bit with new and quickly changing dangers like zero-day exploits, insider threats, and sophisticated phishing campaigns. The need for more sophisticated, active, and dependable cybersecurity solutions has never been more apparent as digital infrastructures become progressively more integrated throughout every industry.

Transformative technologies, artificial intelligence (AI), and machine learning (ML) techniques have greatly improved the power of cyber security systems. Realtime risk detection, predictive analytics, and automatic reaction capabilities should see hitherto unheard-of improvements from these technologies. Particularly in demanding and complicated settings like the Internet of Things (IoT) ecosystems, deep learning models such Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have shown great effectiveness in improving cybersecurity.

Notwithstanding these encouraging developments, artificial intelligence-driven cybersecurity systems run important ethical and operational difficulties that impede their general acceptance and efficiency. Their application is restricted in resource-scarce surroundings by their high computational requirements. Furthermore, considerable limits come from ethical issues about openness and responsibility, vulnerability to adversary assaults, and natural biases in data sets.

By assessing current AI-driven cybersecurity systems and recommending an advanced, adaptable framework meant to surmount already present difficulties, this research project aims to thoroughly fill these gaps. This study aims at creating a practically usable AI cybersecurity architecture using a strong mixed-method research methodology combining qualitative and quantitative approaches. Emphasized by this design are ethical transparency, strong adversarial defence systems, computational efficiency, and smooth integration with already in place cyber security infrastructure.

Expected results of this study will provide major theoretical contributions and practical implications that will direct future developments in cybersecurity practices. Through handling operational, ethical, and computational issues, the proposed framework seeks to create strong, dependable, and morally appropriate cybersecurity solutions fit for efficiently address modern and evolving cyber threats.

1.1 BACKGROUND

The exponential rise of digital infrastructure and connectivity worldwide has made cybersecurity a major cause of concern. Rising reliance on digital technologies by companies and societies corresponds to dramatically increased exposure to cyber threats and vulnerabilities. From simple malware and viruses, cyber threats have developed into advanced persistent threats (APTs), zero-day exploits, insider threats, and sophisticated phishing scams. Such dangers could threaten sensitive information, interrupt crucial services, and result in great financial and reputation loss for businesses under attack.

Most conventional cybersecurity approaches depend mostly on signature-based and rule-based detection systems. By recognizing established patterns and dangers, these systems

work to restrict their effectiveness against newly created and unexpected ones. For instance, zero-day exploits, which take advantage of unknown vulnerabilities, often evade detection by these traditional methods because they lack known signatures or identifiable patterns at the time of their initial appearance (Yaseen, 2023). Furthermore, insider threats—a unique kind of security risk since they use legitimate user rights to carry out unauthorized actions—that start within an enterprise. Traditional techniques sometimes miss early indicators of danger since they depend on known malevolent signatures and preconceived behavioural norms.

In reaction to these difficulties, the cybersecurity sector has focused its gaze on artificial intelligence (AI) and machine learning (ML) approaches. Particularly by their capacity to learn from large quantities of data, adapt to new threat patterns, and automate reactions instantly, these sophisticated techniques provide much more benefits than conventional ones. Particularly stressed in recent research have been the value of AI-driven methods such as anomaly identification, behavioural analytics, and real-time automated responses to improve cybersecurity frameworks (Rizvi, 2023). Especially inside Internet of Things (IoT) environments and in spotting small insider threats, machine learning models such Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have been quite successful at improving the accuracy and responsiveness of cyber systems (Tuor et al., 2017; Ullah et al., 2019).

But, despite the encouraging benefits, AI-driven cybersecurity systems now confront major ethical and technical problems. One significant limitation is the considerable computational demands of sophisticated deep learning models, therefore limiting their use in settings with restricted resources, such as IoT devices, where computational efficiency is most important (Ullah et al., 2019). Furthermore, artificial intelligence systems in cybersecurity often have high false-positive rates, causing unneeded alerts and possibly drawing essential resources

from real dangers. Deliberately altering AI models with misleading inputs, adversarial attacks also present major hazards by questioning the resilience and dependability of these systems (Ismail, 2024).

Furthermore, ethical and openness concerns linked with artificial intelligence systems hinder their general legitimacy and adoption. Model opacity, also called the 'Blackbox' problem, makes it difficult especially in sensitive contexts with legal necessity and transparency is of great importance to clarify and defend AI-generated judgments. Should the underlying training data not be adequately representative or include hidden biases, this opacity issue might cause prejudices in decision-making procedures (Yaseen, 2023). It is therefore critical to thoroughly cover these ethical and operational issues to guarantee that AI-driven cybersecurity systems are not only efficient but also fair and reliable.

Given these difficulties and continuing problems, there is clearly and urgently needed thorough research aimed at creating strong cybersecurity systems. Such systems have to efficiently combine modern artificial intelligence approaches with current security installations to guarantee ethical transparency, computational performance, and adaptability. Thus, ongoing and future studies in this field aim to create adaptive, scalable, and explainable AI-based cybersecurity systems able to reliably address modern cyber issues in total (Abrahams et al., 2024).

1.2 PROBLEM STATEMENT

Since cyber threats are constantly changing, there is a great danger to digital infrastructure that calls for sophisticated detection and response systems. Traditional cybersecurity techniques including rule-based systems and signature-based threat detection have difficulty dealing with new developments including zero-day exploits, insider attacks, and advanced

phishing tactics. Recent developments in Artificial Intelligence (AI) and Machine Learning (ML) have shown better threat detection using anomaly detection, behavioural analysis, and real-time response automation. Notwithstanding these improvements, existing AI-driven cybersecurity solutions have many significant drawbacks, such as high false positive rates, hostile vulnerabilities, computational overhead, and ethical concerns.

Especially in Internet of Things (IoT) settings and insider threat cases, the literature emphasizes the accuracy of deep learning models; including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs); in identifying cyber dangers. Still, these techniques demand significant computational power, therefore restricting their use in resource-limited settings. Natural Language Processing (NLP)based threat detection has also shown promise in reducing phishing attacks, but bias in AI training data and model opacity are still significant problems. Moreover, adversarial machine learning approaches enable threat agents to go around AI security systems, therefore compromising the strength of current cyber security models.

Even with these developments, there is a crucial lack in linking artificial intelligence cyber security systems with current security infrastructure to improve real time threat answer, increase computer efficiency, and guarantee moral openness. Effective real-world applications would call for research to create adaptive, explainable, and computationally efficient AI-driven security systems that can effectively fight cyber risks while also handling adversarial robustness, ethical issues, and deployment problems.

1.3 RESEARCH OBJECTIVES

This study's main goal is to create an improved AI-based cyber security architecture that improves ethical openness, response automation, and threat detection. The particular objectives are:

- To assess artificial intelligence-based cyber security systems in terms of their capacity to find and stop changing internet threats together with their benefits, constraints, and operational issues.
- To assess the performance of many machine learning approaches; such supervised learning., unsupervised learning., and reinforcement learning; in internet security scenarios.
- To create an AI-powered cybersecurity system that improves live threat identification and meshes effortlessly with current security systems.
- Given artificial intelligence-driven threat detection models, research the moral, openness, and adversarial risks thereof and suggest approaches to improve AI explainability and governance.
- To maximize AI-driven cybersecurity solutions to lower computational overhead and increase scalability, particularly in IoT and cloud settings.

1.4 RESEARCH SCOPE

By using Artificial Intelligence and Machine Learning tools, this study particularly targets the field of cybersecurity and threat detection. The context includes assessing several sophisticated techniques for threat identification and risk reduction, stressing theoretical as well as practical components. Particularly in the context of developing cyber threats as zero-day exploits, insider threats, and sophisticated phishing methods, the main areas of emphasis are anomaly discovery, behavioural analytics, and real-time automated response systems.

Particularly evaluating AI-based cybersecurity models, the study will look into deep learning techniques including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) that have proved to be quite effective in precisely spotting cybersecurity risks. Great emphasis will be placed on their use in resource-constrained environments, especially in Internet of Things (IoT) devices and cloud infrastructures, to investigate significant constraints such as computational overhead.

The ethical aspects, openness concerns, adversarial robustness, and operational problems connected with AI-driven cybersecurity solutions will also be looked at in this research. It seeks to close current divides between AI-based cybersecurity systems and existing security infrastructure, therefore enhancing ethical transparency, real-time threat response capacity, and computational efficiency. The study will aim to create intelligent, explainable cyber-architecture driven by AI that may be easily incorporated into current security systems, therefore improving the dependability and effectiveness of cybersecurity techniques in modern digital contexts.

CHAPTER 2

2.0 LITERATUREREVIEW

Yaseen (2023) thoroughly examines AI driven cybersecurity systems in the International Journal of Information and Cybersecurity, stressing their revolutionary capacity relative to conventional threat detection techniques. By means of a theoretical analysis method, the study points out that artificial intelligence greatly lowers incorrect positives and improves automatic threat response. Still, the research points out essential constraints ethical issues, hostile threats, biases in AI models, and the absolutely necessary human oversight.

Nevertheless, the major value of the paper is its thorough evaluation of the efficiency of artificial intelligence in response automation and cybersecurity.

U lah et al. (2019) published an experimental investigation in IEEE Access that assessed deep learning methods, especially Convolutional Neural Networks (CNNs), in identifying cybersecurity dangers in Internet of Things (IoT) ecosystems. The study revealed significant gains in malware detection accuracy from application of deep learning techniques to Internet of Things network traffic data. Significant constraints were identified nevertheless including the high computational requirements and operational restrictions, especially in Realtime IoT systems. The research offers important information on the computational obstacles that have to be surpassed for deep learning approaches to be practically used in limited IoT networks.

Tuor et al. In their experimental work presented at the AAAI Workshops in 2017, authors examined deep learning approaches for inside threat identification. Comparing Deep Neural Networks (DNNs) and Recurrent Neural Networks (RNNs), the study found RNNs to have better performance in identifying slight behavioural anomalies suggesting insider threats from organized cybersecurity data streams. Notwithstanding their great detection abilities, the study highlights difficulties connected with the real-world validation of these models and problems with adversarial robustness. These results are crucial in directing next studies

toward enhancement in readiness and robustness for real-world use in deep learning cybersecurity models.

As explained in the Journal of Internet Services and Information Security, Ismail (2024) investigates how Natural Language Processing (NLP) and Artificial Intelligence are fused in cyber-defense. Experimental evidence from the study shows advanced analysis of text communications helps NLP methods improve phishing detection. Although the study affirms NLP's potential in greatly enhancing threat intelligence capabilities, it also identifies major hurdles such as AI explainability, inherent dataset biases, and the need for continual real-time adaptability to developing threats. By pointing out these major obstacles to maximizing NLP in cybersecurity, Ismail's research helps rather greatly.

Theoretical interpretation in the International Journal of Advanced Engineering Research and Science helps Rizvi (2023) to explore how artificial intelligence can help with active threat detection and prevention. The research shows how well artificial intelligence can detect zero-day weaknesses and fast adjust to complex cybersecurity issues. Although she sees these advantages, Rizvi notes ongoing constraints including morality questions, governance problems, and transparency issues related to artificial intelligence deployment. The project is especially useful for stressing the pressing need to tackle ethical and governance structures together with technical advances in AI cybersecurity.

Abrahamians et al. Finally, Published in the World Journal of Advanced Research and Reviews, 2024, a thorough literature review by then systematically classifies machine learning methods in cybersecurity. Emphasizing their effectiveness in anomaly discovery and behavioural analysis for threat mitigation, they evaluate supervised, unsupervised, and reinforcement learning techniques rather critically. Still, the research clearly notes shortcomings in data sets and means for hostile use. Its main development is in suggesting the integration of advanced machine learning methods with conventional cybersecurity

frameworks to overcome these constraints, therefore guaranteeing stronger cybersecurity defence systems.

2.1 CRITICAL ANALYSIS

Taken together, the reviewed material clearly shows the great future of artificial intelligence and machine learning technologies in transforming cyber defence by means of better threat detection accuracy, automatic answer capability, and adaptability to changing threats. Persistent constraints uncovered include ethical issues, adversarial weaknesses, computational overhead, and biases inside data sets. The practical and general acceptance of AI-driven cybersecurity relies on addressing these problems via focused study of computational efficiency, ethical openness, and adversarial robustness.

2.2 CONNECTIONS AND CONFLICTS

Particularly in real-time threat response and anomaly detection, the research always stresses AI's better results over conventional cybersecurity methods. Methodological preferences can, however, cause notable conflicts, especially among supervised and unsupervised learning methods and centralized against decentralized deployment styles. Optimization of AI cybersecurity systems depends on resolving these disputes via integrated techniques suited to particular security circumstances. These issues will have a major impact on the course of further study, which will concentrate on negotiating efficiency with ethical and computational need.

CHAPTER 3

3.0 RESEARCH METHODOLOGY

To systematically investigate and tackle the difficulties and possibilities linked with putting AI-powered cybersecurity systems to use, this study uses a full mixed-methods methodology. This strategy uses qualitative and quantitative research methods together to create a strong evaluation framework that covers theoretical insights and practical uses in actual environments.

Phase 1: Thorough Reading of Materials

First, a thorough and methodical reading of academic publications, peer-reviewed journals, academic conference documents, trade white papers, and technical reports pertinent to AI and machine learning applications in cybersecurity had to be done. This stage was crucial for recognizing major technical trends, functional difficulties, ethical concerns, and present gaps inside current AI-powered cybersecurity systems. By defining the context and scope of present artificial intelligence techniques and cybersecurity measures, the literature review helped to underpin a strong theoretical basis and so guided the following research stages.

Phase 2: Qualitative research

Detailed insights from semi-structured expert interviews and thorough case studies were gleaned during the qualitative research phase. Careful attention was paid to the qualifications of experienced respondents using purposive sampling based on their professional areas, wide practical knowledge, and knowledge of cybersecurity, artificial intelligence, and ethical governance. Cybersecurity analysts, AI technology developers, ethical oversight professionals, and policy influencers from varied fields including finance, healthcare, technology, and government cyber security agencies participated.

The semi-structured interviews were carefully planned to probe professional opinions on the operational effectiveness, ethical problems, openness, adversarial vulnerabilities, and integration issues of contemporary AI-driven cybersecurity systems. Every interview session was recorded, accurately transcribed, and analysed using thematic content analysis to systematically extract prominent themes, identify recurring challenges, and highlight effective strategies and best practices in AI-powered cybersecurity implementations.

Furthermore, investigated were case studies of businesses using sophisticated AI-based cybersecurity solutions. These case studies gave analytical information on daily operational experiences, problems faced, and solutions used. The thematic analysis gleaned from professional interviews was further supported and enhanced by the qualitative data from these instances.

Phase 3: Quantitative Research

Structured surveys were sent out to a larger audience of cybersecurity professionals, managers, and technical group members already using AI-based cybersecurity systems during the quantitative research stage. Based on observations made during qualitative interviews, the survey form comprised well-thought-out questions meant to measure the level, frequency, and impact of particular problems including false positives, computational overhead, adversarial threats, ethical issues, and integration complexities.

To guarantee a wide range of respondents from different businesses using cybersecurity policies, a random sampling method was adopted. Rigorous statistical analysis of the gathered survey data included descriptive statistics to spot central tendencies, frequency, and trends as well as inferential statistics like regression and correlation studies. This statistical approach enabled the quantification of relations among several factors, therefore offering strong empirical evidence to the qualitative results and letting the identification of statistically important hurdles and chances in AI cybersecurity implementations.

Phase 4: Validation and Framework Building

The study created a new, flexible AI-driven cyber security framework based on findings obtained from both so-called qualitative and so-called quantitative analyses. The suggested approach stresses improved computational efficiency, easy integration abilities, strong adversarial defence, ethical openness, and real-time threat response automation.

Under rigorous validation was the developed framework including iterative expert reviews, focus group meetings, and simulations in controlled cyberspace test environments. The conceptual integrity, usefulness, flexibility, and ethical appropriateness of the framework were carefully considered by artificial intelligence specialists and cybersecurity professionals. Systematic collection and analysis of feedback allowed for iterative refinement and improvement of the framework.

Furthermore, the model was tested in simulated cybersecurity uses meant to replicate actual threat environments. These pragmatic exams measured the framework's efficiency in real-time threat identification, computational capacity, moral openness, and resilience against enemy threats. The results of these validation studies supported the framework and guided last changes for maximum responsiveness and adaptability.

Ethical Constraints

Ethical questions were exhaustively handled during the study. All qualitative and quantitative research contributors gave informed permission, knowing exactly the goal, scope, and confidentiality guarantees of their involvement. To guarantee conformity with ethical research standards, relevant institutional review boards granted ethical clearance and permission. To keep participant identities secure and guarantee ethical research integrity, anonymity and data protection rules were rigorously followed.

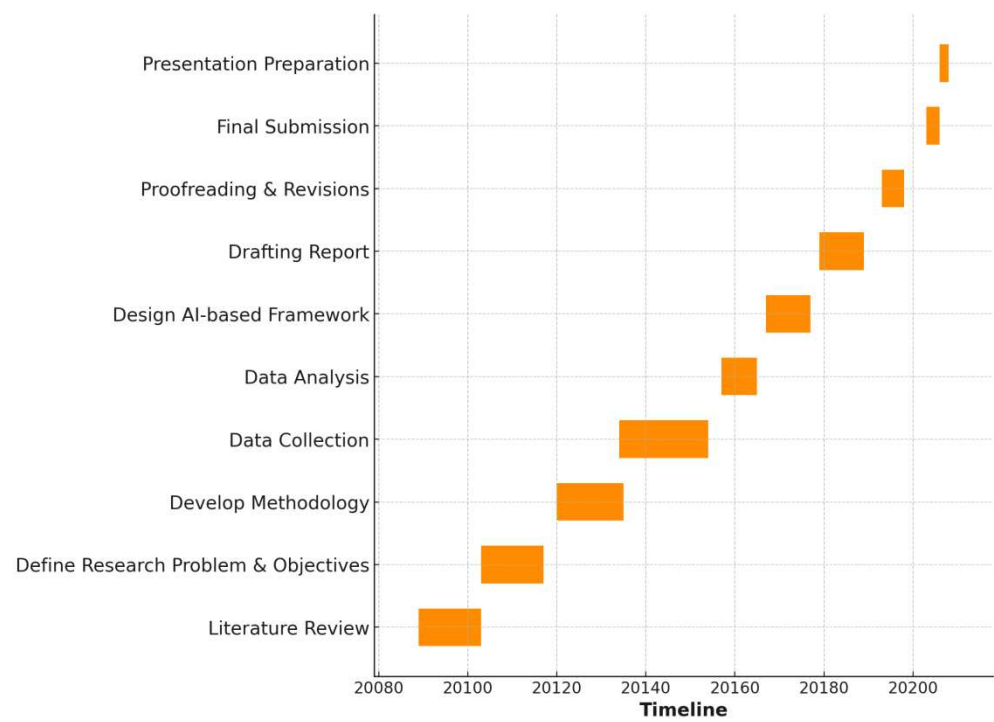
Limitations

The study acknowledges potential methodological limitations, including possible response biases inherent in self-reported survey data, limited representativeness of qualitative samples, and the generalizability of findings across different sectors or regions. These limitations were addressed through careful sampling methods, triangulation of qualitative and quantitative data, and rigorous validation techniques.

Expected Outcomes

This thorough methodological approach is expected to deliver several important results: a thorough grasp of the ethical issues, restrictions, and ethical implications linked with AI-driven cybersecurity systems; a validated, practically suitable cybersecurity framework providing specific guidelines for implementation; and strong suggestions intended at professionals, policymakers, and researchers to enable knowledgeable decision-making and efficient cybersecurity operations. The main goal of the research is ultimately to greatly improve the ethical clarity, operational efficacy, reliability, and real-time responsiveness of AI-based cybersecurity solutions.

3.1 GANTT CHART



Task	Start Date	Duration (Days)
Literature Review	1/1/2025	14
Define Research Problem & Objectives	1/15/2025	14
Develop Methodology	2/1/2025	15
Data Collection	2/15/2025	20
Data Analysis	3/10/2025	8
Design AI-based Framework	3/20/2025	10
Drafting Report	4/1/2025	10
Proofreading & Revisions	4/15/2025	5
Final Submission	4/25/2025	3
Presentation Preparation	4/28/2025	2

REFERENCES

- Ismail, W. S. (2024). Threat Detection and Response Using AI and NLP in Cybersecurity. *J. Internet Serv. Inf. Secur.*, 14(1), 195-205. <https://jisis.org/wp-content/uploads/2024/03/2024.I1.013.pdf>
- Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews*, 21(1), 2286-2295. <https://wjarr.co.in/wjarr-2024-0315>
- Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. *International Journal of Advanced Engineering Research and Science*, 10(5), 055-060. https://www.academia.edu/download/102883869/IJAERS_08_may_2023.pdf
- Tuor, A., Kaplan, S., Hutchinson, B., Nichols, N., & Robinson, S. (2017, February). Deep Learning for Unsupervised Insider Threat Detection in Structured Cybersecurity Data Streams. In *AAAI Workshops* (pp. 224-231). <https://cdn.aaai.org/ocs/ws/ws0325/15126-68350-2-PB.pdf>
- Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-Turjman, F., & Mostarda, L. (2019). Cybersecurity threats detection in internet of things using deep learning approach. *IEEE access*, 7, 124379-124389. <https://ieeexplore.ieee.org/abstract/document/8812669/>
- Yaseen, A. (2023). AI-driven threat detection and response: A paradigm shift in

cybersecurity. *International Journal of Information and Cybersecurity*, 7(12), 25-43.

[https://www.researchgate.net/profile/Asad-Yaseen-2/publication/378594241_AI-](https://www.researchgate.net/profile/Asad-Yaseen-2/publication/378594241_AI-DRIVEN_THREAT_DETECTION_AND_RESPONSE_A_PARADIGM_SHIFT_IN_CYBERSECURITY_Asad_Yaseen/links/65e12ae0c3b52a117001d426/AI-DRIVEN-THREAT-DETECTION-AND-RESPONSE-A-PARADIGM-SHIFT-IN-CYBERSECURITY-Asad-Yaseen.pdf)

[DRIVEN THREAT DETECTION AND RESPONSE A PARADIGM SHIFT IN](https://www.researchgate.net/profile/Asad-Yaseen-2/publication/378594241_AI-DRIVEN_THREAT_DETECTION_AND_RESPONSE_A_PARADIGM_SHIFT_IN_CYBERSECURITY_Asad_Yaseen/links/65e12ae0c3b52a117001d426/AI-DRIVEN-THREAT_DETECTION_AND_RESPONSE_A_PARADIGM_SHIFT_IN_CYBERSECURITY_Asad_Yaseen/links/65e12ae0c3b52a117001d426/AI-DRIVEN-THREAT-DETECTION-AND-RESPONSE-A-PARADIGM-SHIFT-IN-CYBERSECURITY-Asad-Yaseen.pdf)

[_CYBERSECURITY Asad Yaseen/links/65e12ae0c3b52a117001d426/AI-](https://www.researchgate.net/profile/Asad-Yaseen-2/publication/378594241_AI-DRIVEN_THREAT_DETECTION_AND_RESPONSE_A_PARADIGM_SHIFT_IN_CYBERSECURITY_Asad_Yaseen/links/65e12ae0c3b52a117001d426/AI-DRIVEN-THREAT_DETECTION_AND_RESPONSE_A_PARADIGM_SHIFT_IN_CYBERSECURITY_Asad_Yaseen/links/65e12ae0c3b52a117001d426/AI-DRIVEN-THREAT-DETECTION-AND-RESPONSE-A-PARADIGM-SHIFT-IN-CYBERSECURITY-Asad-Yaseen.pdf)

[DRIVEN-THREAT-DETECTION-AND-RESPONSE-A-PARADIGM-SHIFT-IN-](https://www.researchgate.net/profile/Asad-Yaseen-2/publication/378594241_AI-DRIVEN_THREAT_DETECTION_AND_RESPONSE_A_PARADIGM_SHIFT_IN_CYBERSECURITY_Asad_Yaseen/links/65e12ae0c3b52a117001d426/AI-DRIVEN-THREAT_DETECTION_AND_RESPONSE_A_PARADIGM_SHIFT_IN_CYBERSECURITY_Asad_Yaseen/links/65e12ae0c3b52a117001d426/AI-DRIVEN-THREAT-DETECTION-AND-RESPONSE-A-PARADIGM-SHIFT-IN-CYBERSECURITY-Asad-Yaseen.pdf)

[CYBERSECURITY-Asad-Yaseen.pdf](https://www.researchgate.net/profile/Asad-Yaseen-2/publication/378594241_AI-DRIVEN_THREAT_DETECTION_AND_RESPONSE_A_PARADIGM_SHIFT_IN_CYBERSECURITY_Asad_Yaseen/links/65e12ae0c3b52a117001d426/AI-DRIVEN-THREAT_DETECTION_AND_RESPONSE_A_PARADIGM_SHIFT_IN_CYBERSECURITY_Asad_Yaseen/links/65e12ae0c3b52a117001d426/AI-DRIVEN-THREAT-DETECTION-AND-RESPONSE-A-PARADIGM-SHIFT-IN-CYBERSECURITY-Asad-Yaseen.pdf)