IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

A Study on AI's Potential in Combating Cybercrimes through Real-Time Detection and Response to Fraudulent Activities.

Kathaniya K
B.B.A, LLB.(Hons.)
Saveetha School of Law, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai
kathanyakathan1123@gmail.com

Abstract: *Artificial Intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions. The research method followed is empirical research. A convenience sampling is a sample where the respondents are selected, in part or in whole, at the convenience of the researcher and data was collected by a structured questionnaire. The samples were collected from friends and relatives as well as nearby college and public. Sample size is 200. The questionnaires consisted of demographic data and statements in Likert scale. The independent variables are gender, age, occupation, educational qualification, income and marital status. The dependent variables are Real-time AI monitoring is used to detect and responses to fraudulent activities and its ethical concerns helps to Combating cybercrimes, collaboration between humans and AI is the best approach for addressing cybercrime, On a scale of (1 to 5)how concerned are you about the ethical implications of AI in cybersecurity, organizations Should prioritize ethical considerations when implementing AI for cybersecurity. Primary advantage of using AI in combating cybercrimes, Regulations should govern the use of AI in cybersecurity. All data was analyzed by using the SPSS tool. AI systems fail to prevent cyberattacks, Organizations need to be open to adopting new technologies and embracing change, Continuous research and development are needed to improve the accuracy in cybersecurity and efficiency of AI algorithms. Findings about Artificial Intelligence (AI) has emerged as a powerful tool in the fight against cybercrime. Its ability to analyze vast amounts of data in real-time and identify patterns that might be missed by human analysts makes it a valuable asset in detecting and responding to fraudulent activities..*

Keywords: cybercrime, Organizations, cybersecurity, Artificial Intelligence, collaboration

I. INTRODUCTION

Overview: Artificial Intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions. These machines are trained on vast amounts of data to recognize patterns, make decisions, and solve problems. The Main **Aim** of this Study is how the potential of AI is Innovating cybersecurity by exploring its application in real-time detection and response to fraudulent activities.The **objective** of this research is to explore how Artificial Intelligence (AI) can be effectively used to enhance cybersecurity measures, particularly in the realm of real-time detection and response to fraudulent activities.AI that is capable of understanding or learning any intellectual task that a human being can.

Evolution: From sophisticated phishing attacks to large-scale data breaches, malicious actors continually exploit vulnerabilities in systems and networks. By leveraging advanced algorithms and machine learning techniques, AI can identify patterns, anomalies, and potential threats that may go unnoticed by human analysts.

Government initiatives have accelerated AI adoption across various sectors National Strategy for Artificial Intelligence: This strategy outlines a comprehensive vision for India's AI development, including its application in cybersecurity and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 9, June 2025 Impact Factor: 7.67

Public-Private Partnerships: The government has fostered collaborations between public and private sectors to develop innovative AI-based cybersecurity solutions.

Factors affecting are **Privacy Concerns:** AI systems may collect and process sensitive personal data, raising privacy concerns,Organizations may face legal consequences if AI systems fail to prevent cyberattacks,Organizations need to be open to adopting new technologies and embracing change,Continuous research and development are needed to improve the accuracy and efficiency of AI algorithms.

Current trends are AI can automate routine tasks, such as blocking malicious IP addresses and initiating incident response protocols, **Behavioral Analytics:** AI can analyze user behavior patterns to identify anomalies and potential threats.AI-powered systems can detect and respond to threats in real-time, reducing the impact of attacks.

Comparing countries India has a large pool of skilled AI and machine learning professionals , The Chinese government has prioritized AI development and has implemented ambitious plans to become a global leader in AI.

OBJECTIVES:

- To understand the way Real-time AI monitoring is used to detect and respond to fraudulent activities .
- To Analyse people concerned about the ethical implications of AI in cybersecurity.
- To Examine collaboration between humans and AI is the best approach for addressing cybercrime.

II. REVIEW OF LITERATURE

Oluwabusayo Adijat Bello1 & Komolafe Olufemi(2024) Artificial Intelligence (AI) offers innovative solutions to thisgrowing problem, leveraging its ability to analyze vast amounts of data, identify patterns, and predict fraudulent behavior with high accuracy. This abstract explores the various AI techniques and their applications in fraud prevention, highlighting their transformative impact on the security landscape. AI techniques such as machine learning (ML), deep learning, and natural language processing (NLP) have revolutionized fraud detection and prevention. Machine learning algorithms, particularly supervised learning models like decision trees and neural networks, areused extensively to identify fraudulent transactions by learning from historical data.

Onuh Matthew Ijiga 1, Idoko Peter Idoko (2024) This paper explores the integration of Artificial Intelligence (AI) and AdversarialMachine Learning (ML) techniques as a formidable strategy against increasingly sophisticated cyber-attacks. We present a comprehensive framework that leverages AI to dynamically assess cybersecurity risks and detect fraudulent activities with unprecedented accuracy and speed.Firstly, we delve into the foundational principles of adversarialmachine learning, outlining how these techniques can be employed to simulate potential cyber threats, thereby enablingthe development of more resilient AI-driven cybersecurity systems.

Selma Dilek, Hüseyin Çakır, Mustafa Aydın(2015) Advances in information technology (IT) criminals are using cyberspace to commit numerous cyber crimes. Cyber infrastructures are highly vulnerable to intrusions and other threats. Physical devices and human intervention are not sufficient for monitoring and protection of these infrastructures; hence, there is a need for more sophisticated cyber defense systems that need to be flexible, adaptable and robust, and able to detect a wide variety of threats and make intelligent real-time decisions. Numerous bio-inspired computing methods of Artificial Intelligence have been increasingly playing an important role in cyber crime detection and prevention.

Sonam Rani ; Ajit Mittal (2023)concentrating on instantaneous transaction surveillance and irregularity detection, as crucial elements of safeguarding digital payments. The investigation embraces a comparative exploration blueprint, examining and amalgamating pertinent articles and research papers issued from 2010 to 2023. This investigation depends on auxiliary data sources, particularly articles and scholarly papers, to offer perspectives into the progressions, efficiency, and obstacles of AI-powered deception identification in the setting of digital payment safety.

Ahmad Abdulqadir Al Rababah(2024) Developments in artificial intelligence and big data analytics have significantly contributed to combating cybercrime and enhancing digital citizenship. By using AI technologies such as machine learning and artificial neural networks, large datasets can be analyzed quickly and accurately to detect patterns of fraud and suspicious online activities. For example, AI can be used to identify abnormal behaviors online, such as banking fraud or data breaches, allowing for rapid intervention to prevent crimes before they occur. Additionally, big

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 9, June 2025 Impact Factor: 7.67

data analysis can be used to track crime patterns and identify geographic areas at risk of cybercrime, helping to guide development and training efforts for police forces and enhance digital security for citizens.

Iqra Naseer (2024) Cyber and phishing assaults are becoming more common and complex, and artificial intelligence (AI) hasbecome an essential tool for detecting and blocking them. This study delves into the ways AI-driven solutionsmight improve cybersecurity by spotting possible threats in real-time using machine learning techniques, naturallanguage processing, and pattern recognition. AI enables early detection of anomalies in network traffic,recognizing phishing emails, malicious URLs, and suspicious behaviors that may go unnoticed by traditionalmethods. Also, AI can learn from new threats all the time, so it can better defend itself, which means fewer false positives and better security standards overall.

Hamed Taherdoost(2024) Hamed Taherdoost Amidst an unprecedented period of technological progress, incorporating digital platforms into diverse domains of existence has become indispensable, fundamentally altering the operational processes of governments, businesses, and individuals. Nevertheless, the swift process of digitization has concurrently led to the emergence of cybercrime, which takes advantage of weaknesses in interconnected systems. The growing dependence of society on digital communication, commerce, and information sharing has led to the exploitation of these platforms by malicious actors for hacking, identity theft, ransomware, and phishing attacks. With the growing dependence of organizations, businesses, and individuals on digital platforms for information exchange, commerce, and communication, malicious actors have identified the susceptibilities present in these systems and have begun to exploit them.

Gupta, Pankaj (2024) conducting an extensive examination of existing literature and analysing numerous case studies to gather information on the role of artificial intelligence, data, and analytics in fraud prevention.investigates the interconnections among Data Analytics, Artificial Intelligence, and other cutting-edge technologies to enhance comprehension of fraud prevention. The advantages of integrating machine learning and data analytics into artificial intelligence systems for industry-wide fraud detection and prevention are examined in this study.the various ways in which analytics, data, and artificial intelligence can be implemented to prevent fraudulent activities. An examination of comparisons between generative AI for social engineering, credit card analytics, and cyber-physical security for Internet of Things (IoT) networks illuminated the merits and demerits of different Artificial Intelligence (AI) approaches.

Olakunle Abayomi Ajala(2024) The contemporary cybersecurity landscape demands innovative solutions to combat the relentless evolution of cyber threats. Traditional approaches are facing unprecedented challenges, compelling a paradigm shift towards the integration of Artificial Intelligence (AI) and Machine Learning (ML). This paper meticulously explores the potential of AI and ML to fortify real-time cybersecurity, with a focus on the swift prediction and mitigation of cyber-attacks. Against the backdrop of an escalating threat landscape, this paper propels the inquiry into advanced technologies to fortify cybersecurity. The limitations of traditional methodologies underscore the urgency of investigating the efficacy of AI and ML in reinforcing defense mechanisms.

Damian Puchalski(2024)the increasing sophistication and proliferation of cyberthreats have underscored the necessity for robust network security measures, as well as a comprehensive approach to cyberprotection at large. As cyberthreats are continuously more and more complex, and their detection, response and mitigation often involve dealing with big data, the need for novel solutions is present also in cyber-criminal law enforcement (LEA) and network forensics contexts. Traditional, anomaly-based or signature-based intrusion detection systems (IDS) often face challenges in adapting to the evolving cyberattack landscape.

Paschal Uchenna Chinedu(2021) As virulent and damaging as it is, cybercrime is also the most complicated globalized crime of the 21st century. The menace is felt and appreciated across different jurisdictions. In the last two decades, it has been interestingly observed that as advanced and supposed secure information technologies are deployed in the cyberspace their hidden vulnerabilities are promptly uncoveredunconscionably following exploits by not only attackers but hobbyistsand cybersecurity apologists who are either interested in discovering the vulnerabilities .To curb this menace, different approaches have been adopted including political, legislative, social, economic and technology-based solutions. Technology-based solutions for combatting cybercrime have been in the forefront and may be categorized into intelligent, traditional, and hybrid solutions.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

Fatema Tuz johara(2023) Conventional rule-based fraud detection strategies have struggled to keep pace with the rapid evolution of cyber threats, prompting a surge of interest in more adaptive approaches like unsupervised learning. Furthermore, the COVID-19 pandemic has exacerbated the issue of bank fraud due to the widespread transition to online platforms and the proliferation of charitable funds, which present ripe opportunities for exploitation by cybercriminals. In response to these pressing concerns, this study delves into the realm of machine learning algorithms for the analysis and identification of fraudulent banking transactions.

Mahfujur Rahman Faraji1(2024) Artificial intelligence (AI) is a powerful technology that helps cybersecurity teams automate repetitive tasks, accelerate threat detection and response, and improve the accuracy of their actions to strengthen their security posture against various security issues and cyberattacks. This objective focuses on analysing how AI-based cyber security (CS) solutions improve performance in financial transactions and banking sectors. It also aims to identify the latest advancements in AI-driven CS) research to enhance security and operational efficiency in the financial sector. This article presents a systematic literature review and a detailed analysis of AI use cases for cybersecurity in financial transactions. The review resulted in 800 studies, of which 225 articles remain. This paper will provide readers with a comprehensive overview of the potential of AI to improve cybersecurity in financial transactions. The review also identifies future research opportunities in examining cybersecurity application areas.

Jack nicolls(2024) Machine Learning and Deep Learning methods are widely adopted across financial domains to support trading activities, mobile banking, payments, and making customer credit decisions. These methods also play a vital role in combating financial crime, fraud, and cyberattacks. Financial crime is increasingly being committed over cyberspace, and cybercriminals are using a combination of hacking and social engineering techniques which are bypassing current financial and corporate institution security. With this comes a new umbrella term to capture the evolving landscape which is financial cybercrime. It is a combination of financial crime, hacking, and social engineering committed over cyberspace for the sole purpose of illegal economic gain. Identifying financial cybercrime-related activities is a hard problem, for example, a highly restrictive algorithm may block all suspicious activity obstructing genuine customer business.

Massimiliano Aschi(2022) Frauds in financial services are an ever-increasing phenomenon, and cybercrime generates multimillion revenues, therefore even a small improvement in fraud detection rates would generate significant savings. This chapter arises from the need to overcome the limitations of the rule-based systems to block potentially fraudulent transactions. After mentioning the limitations of rule-based approach, this chapter explains how machine learning is able to address many of these limitations and, more effectively, identify risky transactions.

Faisal S.Alsubaei(2024) Protecting against interference is essential at a time when wireless communications are essential for sending large amounts of data. Our research presents a novel deep learning technique, the ResNeXt method and embedded Gated Recurrent Unit (GRU) model (RNT), rigorously developed for real-time phishing attack detection. Focused on countering the escalating threat of phishing assaults and bolstering digital forensics, our systematic approach involves SMOTE for managing data imbalance during initial data processing. The model's discriminative capability is improved, particularly in the feature extraction process, when autoencoders and ResNet (EARN) are integrated with feature engineering.

Balamurugan M. (2024) This paper examines the high-stakes digital duel between fraudsters wielding GAI and the adaptive defense mechanisms of financial institutions. The paper explores how GAI-created synthetic identities challenge traditional fraud detection paradigms with convincing backstories, digital footprints, and AI-generated images. These artificial personas'unprecedented scale and sophistication threaten to overwhelm existing security infrastructures, potentially compromising the integrity of financial systems and identity verification frameworks. Our analysis revealslarge-scale synthetic identity campaigns' far-reaching economic implications and disruptive potential across multiple sectors.

Amir Djenna (2023) Cybercriminals are becoming increasingly intelligent and aggressive, making them more adept at covering their tracks, and the global epidemic of cybercrime necessitates significant efforts to enhance cybersecurity in a realistic way. The COVID-19 pandemic has accelerated the cybercrime threat landscape. Cybercrime has a significant impact on the gross domestic product (GDP) of every targeted country. It encompasses a broad spectrum of offenses committed online, including hacking; sensitive information theft; phishing; online fraud; modern malware distribution;

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

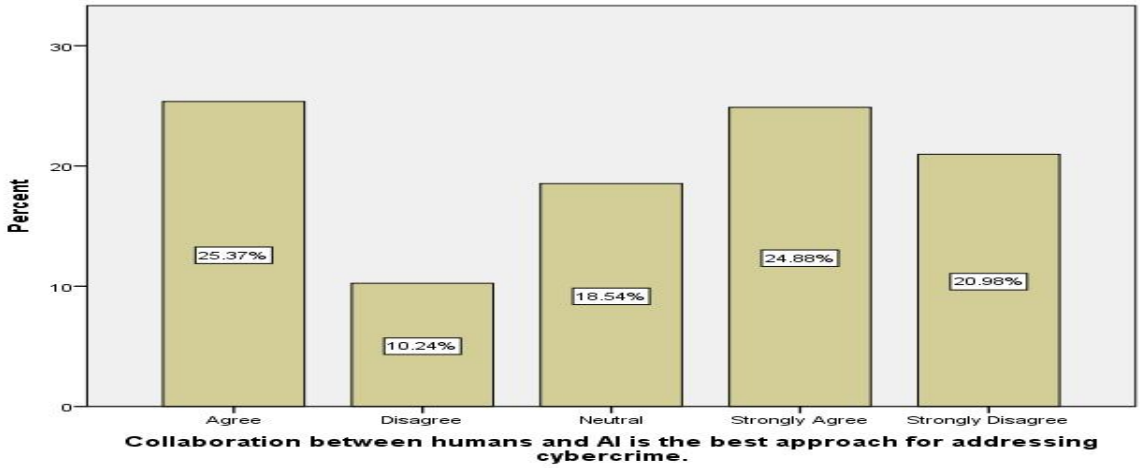
cyberbullying; cyber espionage; and notably, cyberattacks orchestrated by botnets. This study provides a new collaborative deep learning approach based on unsupervised long short-term memory (LSTM) and supervised convolutional neural network (CNN) models for the early identification and detection of botnet attacks.

Oluwabusayo Adijat (2023) Fraud prevention in financial transactions has become increasingly critical as digital payment methods proliferate and cybercriminals employ more sophisticated techniques. Traditional rule-based systems, while still in use, often fall short in detecting complex and evolving fraud patterns. Machine Learning (ML) approaches offer a robust alternative, providing dynamic and adaptive solutions to enhance fraud prevention. This abstract explores various ML techniques employed in the financial sector to mitigate fraud risks. Supervised learning models, such as logistic regression, decision trees, and neural networks, are widely used for fraud detection.

Kodete, Chandra Shikhi (2024) The alarming security threats in the internet world continually raise critical concerns among individuals, organizations and governments alike. The sophistication of cyber-attacks makes it imperative for a paradigm shift from traditional approaches and measures for quelling the attacks to modern sophisticated, digital and strategic ones, such as those involving machine learning and other technologies of artificial intelligence (AI). This study is aimed at examining machine learning (ML) strategies for effective cyber security. ML involves using algorithms and statistical models to enable computers learn from and make decisions or predictions based on data. The study relied on secondary data, which were subjected to a systematic review.

IV. ANALYSIS

Figure :01



LEGEND: Figure 01 Represents the Collaboration between humans and AI is the best approach for addressing cybercrime .

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

Figure :02

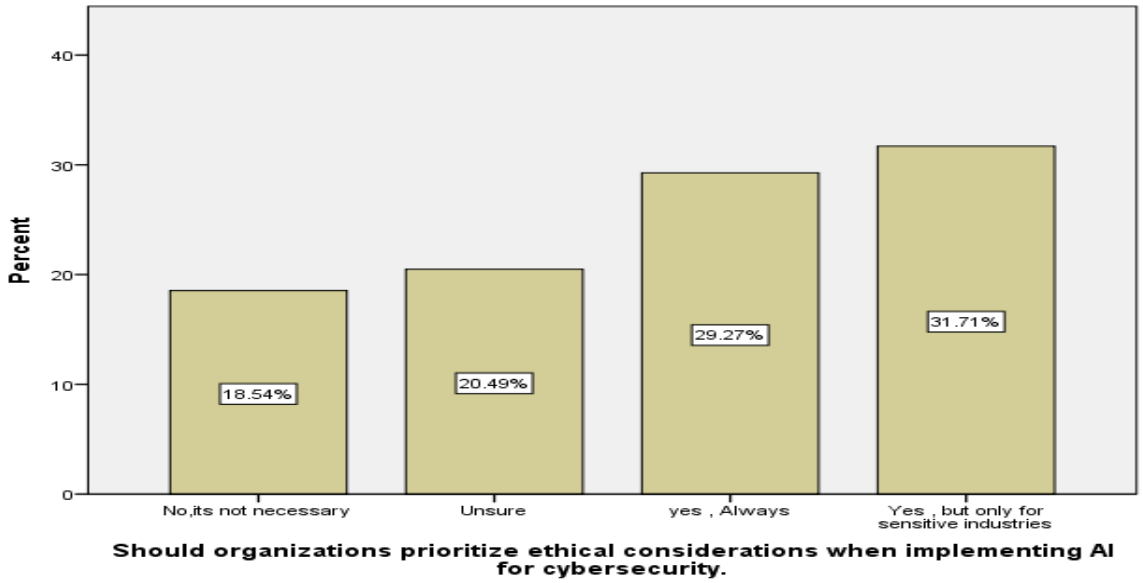


Figure 02 Represents the should the organisations prioritize ethical considerations when implementing AI for cyber security.

Figure :03

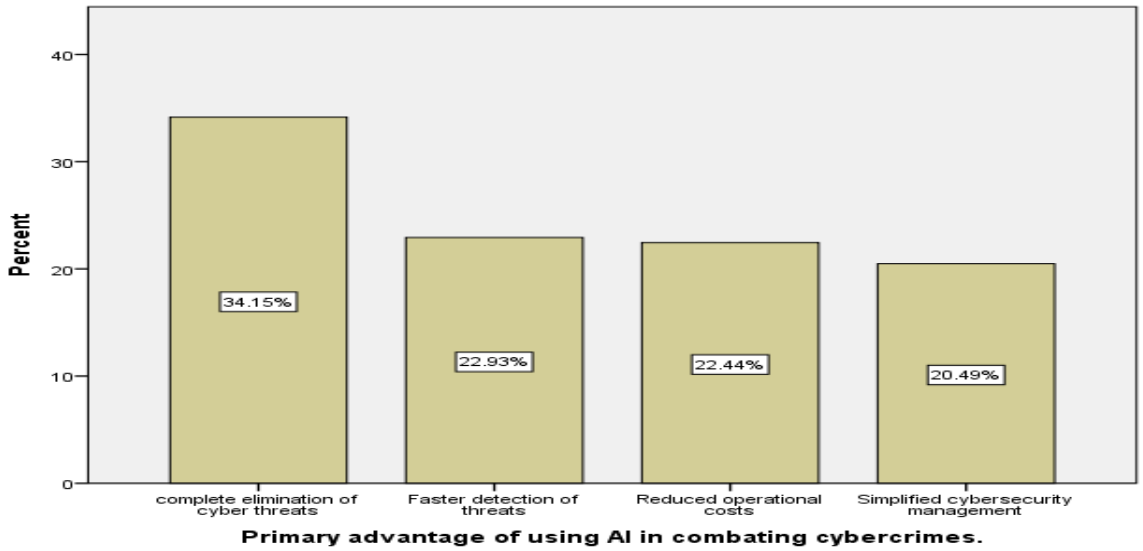


Figure 03 Represents the primary advantage of using AI in combating cybercrimes.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

Figure 04:

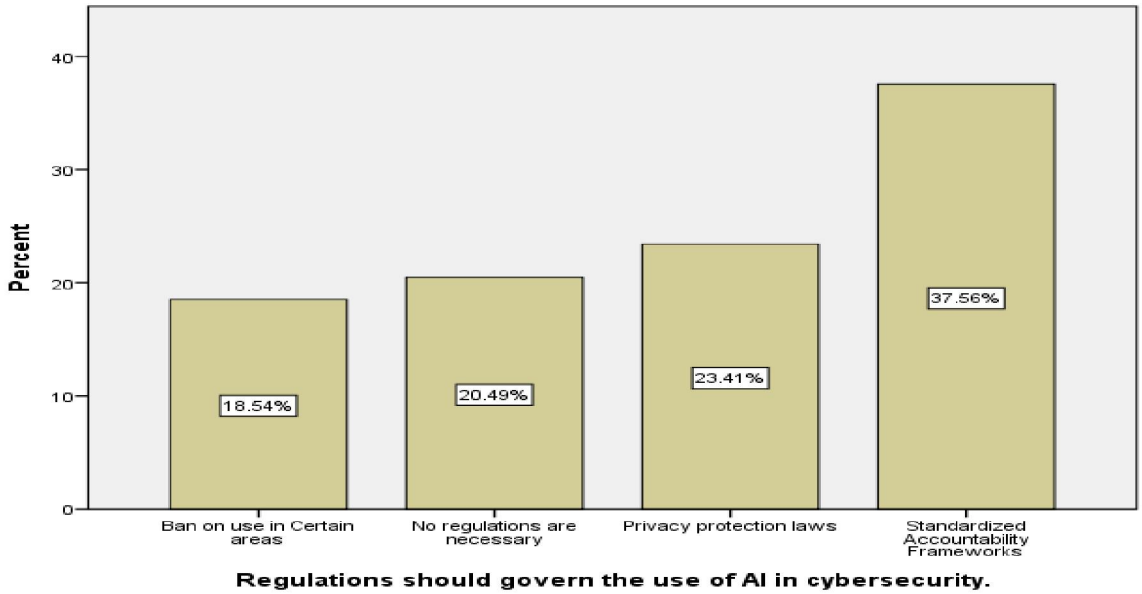


Figure 04 Represents the Regulations that govern the use of AI in cybersecurity.

Figure:05

Figure 05 Represents the Real-time AI monitoring is used to detect and respond to fraudulent activities and its ethical concerns helps to combat cybercrimes.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

Figure 06:

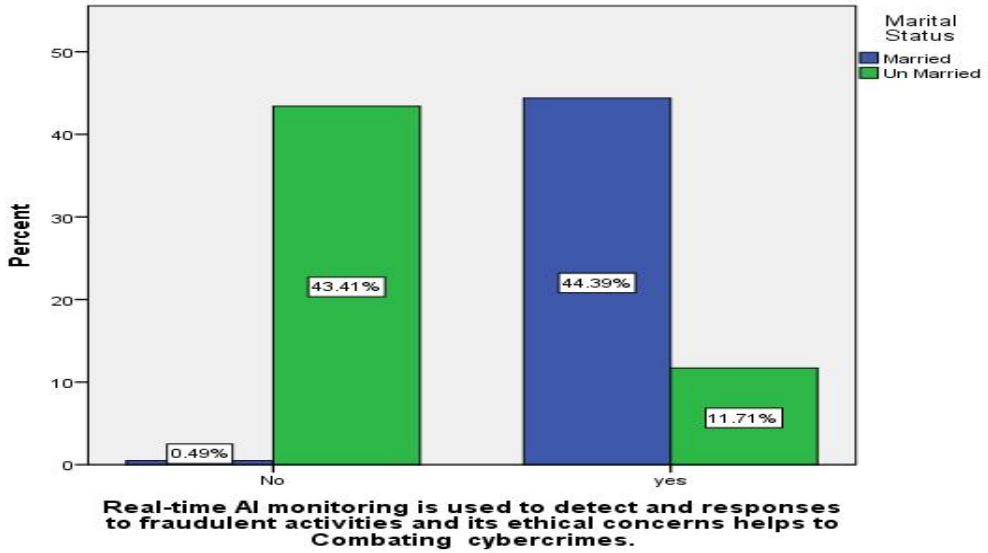


Figure 06 Represents the Real-time AI monitoring is used to detect and respond to fraudulent activities and its ethical concerns helps to combat cybercrimes.

Figure 07:

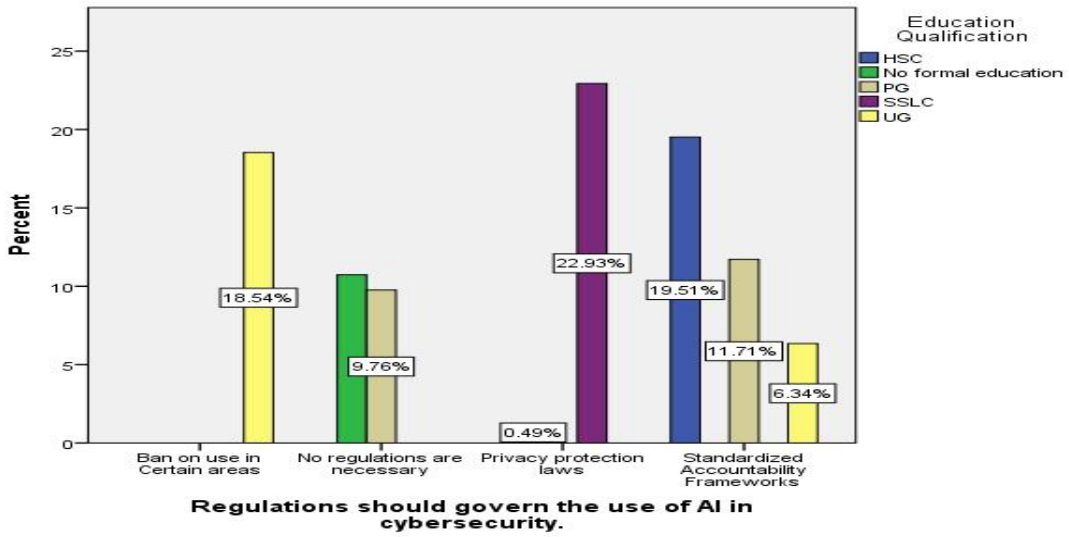


Figure 07 Represents the Real-time AI monitoring is used to detect and respond to fraudulent activities and its ethical concerns helps to combat cybercrimes with respect to their qualification.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

Figure 08:

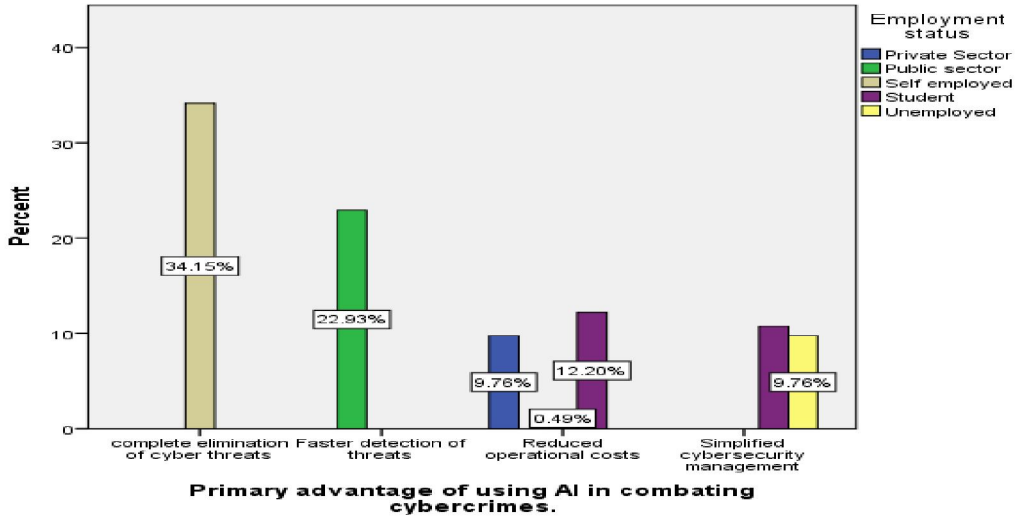


Figure 08 Represents the primary advantage of using AI in combating cybercrimes with respect to their Employment status.

Figure 09:

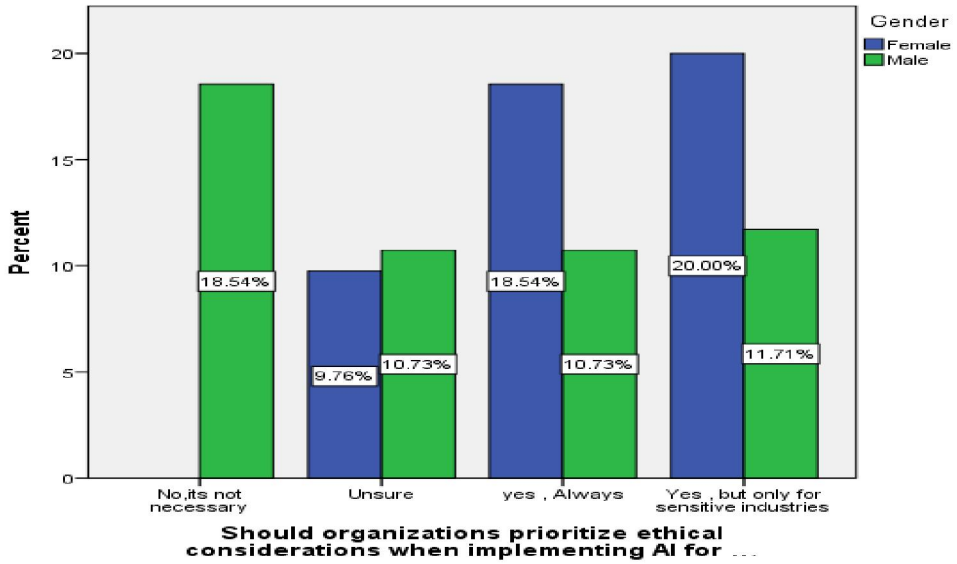


Figure 09 Represents the organizations prioritize ethical considerations when implementing AI for cyber security with respect to their Gender.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

Figure 10:

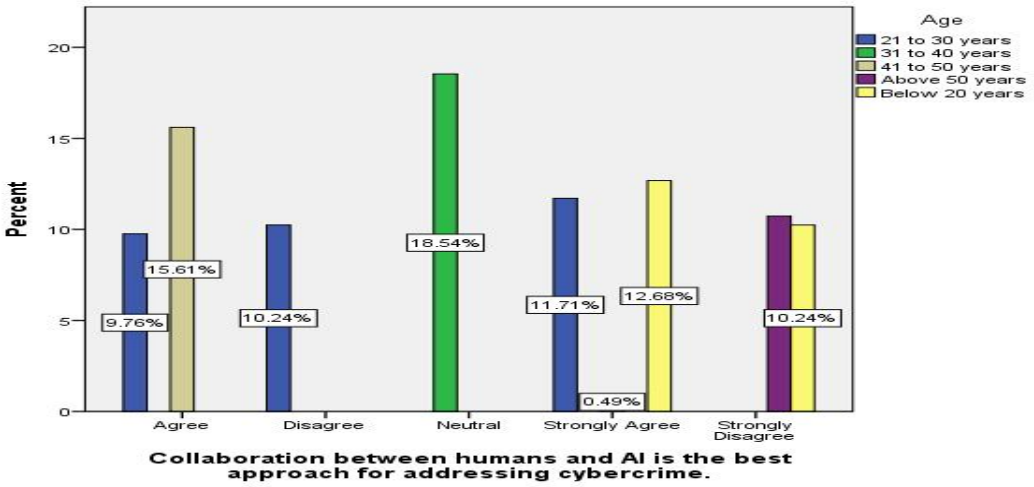


Figure 10 Represents the collaboration between humans and AI is the approach for addressing cybercrime with respect to their Age.

V. RESULT

Figure 01 clearly shows that People are agree that Collaboration between humans and AI is the best approach for addressing cybercrime.

Figure 02 clearly shows that people are supported that organisations should prioritize ethical considerations when implementing AI for cybersecurity only for sensitive industries.

Figure 03 clearly shows that people are given their opinion that complete elimination of cyber threats is the primary advantage of using AI in combating cybercrimes.

Figure 04 clearly shows that people highly support that Regulations should govern the use of AI in cybersecurity in the way of standardized Accountability Frameworks.

Figure 05 clearly shows that people agree that Real-time AI Monitoring is used to detect and respond to fraudulent activities and its ethical concerns help to combat cybercrimes.

Figure 06 clearly shows that Married Couples Agree about Real-time monitoring is used to detect and respond to fraudulent activities and its ethical concerns helps to combat cyber crimes.

Figure 07 clearly shows that SSLC students highly responded that privacy protection laws regulations should govern the use of AI in cybersecurity.

Figure 08 clearly shows that self employed people are highly responsible for complete elimination of cyber threats. This is the primary advantage of using AI in combating cybercrimes.

Figure 09 clearly shows that Female gender says that only for sensitive industries organisations should prioritise ethical consideration when implementing AI for cyber security.

Figure 10 clearly shows that people between the ages of 31 to 40 years are highly in agreement about collaboration between humans and AI is the best approach for addressing. cybercrime.

VI. DISCUSSION

Figure 01 Represents People agree that collaboration between humans and AI is the best approach for addressing cybercrime because it combines the strengths of both human intelligence and machine efficiency because AI can process vast amounts of data quickly, identifying patterns and threats in real-time that would be impossible for humans to detect manually. This rapid response is crucial in countering fast-evolving cyberattacks.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 9, June 2025 Impact Factor: 7.67

Figure 02 Represents People support the idea that organizations should prioritize ethical considerations when implementing AI for cybersecurity, especially in sensitive industries because Sensitive industries, such as healthcare, finance, and government, deal with highly personal or confidential data. AI systems in these sectors must be designed to safeguard individuals' privacy and ensure compliance with regulations. Without proper ethical oversight, AI could inadvertently expose or misuse sensitive data.

Figure 03 Represents people who are given their opinion that complete elimination of cyber threats is the primary advantage of using AI in combating cybercrimes because AI can detect, analyze, and respond to cyber threats much faster than humans. Its ability to process large volumes of data and identify patterns in real-time significantly reduces the window of opportunity for cybercriminals to cause damage.

Figure 04 Represents People strongly support the idea that regulations should govern the use of AI in cybersecurity through standardized accountability frameworks because AI in cybersecurity can be a double-edged sword. While it enhances threat detection and response, it can also be exploited for malicious purposes (e.g., automated hacking tools). Standardized accountability frameworks ensure proper usage by setting clear rules on how AI is developed, deployed, and monitored.

Figure 05 Represents People agree that real-time AI monitoring is crucial for detecting and responding to fraudulent activities and that addressing its ethical concerns can help combat cybercrimes effectively **:** AI can monitor and analyze millions of activities simultaneously, which would be impossible for human teams to achieve at the same speed and scale.Real-time AI monitoring systems with transparent algorithms enable organizations to explain and justify actions taken in response to suspected fraud.

Figure 06 Represents Married couples may agree that real-time monitoring for detecting and responding to fraudulent activities is essential, and addressing its ethical concern**s** helps combat cybercrimes effectively Cybercrimes can target personal or family information, such as addresses, health records, or children's data. Real-time monitoring provides a protective layer, ensuring these details remain secure.. Real-time monitoring can protect their combined assets by quickly identifying fraudulent transactions or unauthorized access.

Figure 07 Represents SSLC (Secondary School Leaving Certificate) students may highly support privacy protection laws and regulations governing the use of AI in cybersecurity SSLC students frequently use digital platforms for education, social media, and entertainment. They recognize the importance of protecting their personal information from being exploited or misused. With growing awareness of cyber threats like data breaches and identity theft, students see the need for regulations to ensure AI systems respect their privacy.

Figure 08 Represents Self-employed people are highly responsible for ensuring the complete elimination of cyber threats because they often bear sole responsibility for their business's security. The primary advantage of using AI in combating cybercrimes is its ability to address this challenge effectively , Self-employed individuals typically lack the resources to hire cybersecurity experts, making them solely responsible for protecting their digital assets.

Figure 09 Represents The female perspective that organizations in sensitive industries should prioritize ethical considerations when implementing AI for cybersecurity , Sensitive industries such as healthcare, finance, or defense handle critical and personal information (e.g., medical records, financial data, national security). Women often emphasize the need to prevent AI biases, especially in industries like law enforcement, where ethical lapses can lead to profiling or unfair targeting.

Figure 10 Represents the ages of 31 to 40 years often agree that collaboration between humans and AI This age group has grown up with evolving technology and is comfortable leveraging AI for cybersecurity. However, they are also aware of its limitations, such as biases or errors in judgment , They value human intervention to interpret AI findings, make nuanced decisions, and ensure ethical practices in combating cybercrime.

VII. RESEARCH METHODOLOGY

The research method followed is empirical research. A convenience sampling is a sample where the respondents are selected, in part or in whole, at the convenience of the researcher and data was collected by a structured questionnaire. The samples were collected from friends and relatives as well as nearby college and public. Sample size is 200. The questionnaires consisted of demographic data and statements in Likert scale. The independent variables are gender, age,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

occupation, educational qualification, income and marital status. The dependent variables are Real-time AI monitoring is used to detect and responses to fraudulent activities and its ethical concerns helps to Combating cybercrimes, collaboration between humans and AI is the best approach for addressing cybercrime, On a scale of (1 to 5)how concerned are you about the ethical implications of AI in cybersecurity, organizations Should prioritize ethical considerations when implementing AI for cybersecurity. Primary advantage of using AI in combating cybercrimes, Regulations should govern the use of AI in cybersecurity. All data was analyzed by using the SPSS tool.

LIMITATIONS:

One of the major limitations of the study is the sample frame.There is a major constraint in the sample frame as it is limited to the smaller area.Thus, it proves to be difficult to extrapolate it to a larger population.Another limitation is the sample size of 200 which cannot be used to assume the thinking of the entire population in a particular country, state, or city. The physical factors have a larger impact, thus, limiting the study.

VIII. CONCLUSION

AI that is capable of understanding or learning any intellectual task that a human being can. In today's increasingly digital world, cybercrime has emerged as a significant global challenge. From sophisticated phishing attacks to large-scale data breaches, malicious actors continually exploit vulnerabilities in systems and networks. objective is to By addressing these challenges and harnessing the power of AI responsibly, we can build a more resilient digital future, where cybercrime is no longer a pervasive threat. The research method followed is empirical research. A convenience sampling is a sample where the respondents are selected, in part or in whole, at the convenience of the researcher and data was collected by a structured questionnaire. The samples were collected from friends and relatives as well as nearby college and public. **Findings** about Artificial Intelligence (AI) has emerged as a powerful tool in the fight against cybercrime. People strongly support the idea that regulations should govern the use of AI in cybersecurity through standardized accountability frameworks because AI in cybersecurity can be a double-edged sword. While it enhances threat detection and response, it can also be exploited for malicious purposes (e.g., automated hacking tools). Standardized accountability frameworks ensure proper usage by setting clear rules on how AI is developed, deployed, and monitored.

REFERENCES

[1]. Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. Computer Science & IT Research Journal, 5(6), 1505–1520. doi:10.51594/csitrj.v5i6.1252

[2]. Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. Open Access Research Journal of Science and Technology, 11(1), 001–004. doi:10.53022/oarjst.2024.11.1.0060

[3]. Dilek, S., Çakır, H., & Aydın, M. (2015). 19 pages, a survey. Artificial Intelligence (Cs.AI); Cryptography and Security (Cs.CR); Computers and Society, 6. doi:10.5121/ijaia.2015.6102

[4]. Rani, S., & Mittal, A. (2023, September 14). Securing digital payments a comprehensive analysis of AI driven fraud detection with real time transaction monitoring and anomaly detection. 2023 6th International Conference on Contemporary Computing and Informatics (IC3I). Presented at the 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), Gautam Buddha Nagar, India. doi:10.1109/ic3i59117.2023.10397958

[5]. Ahmad Abdulqadir Al Rababah(2024)International journal of science academic research. (n.d.). Retrieved 6 December 2024, from http://www.scienceijsar.com.

[6]. Naseer, I. (2024). The role of artificial intelligence in detecting and preventing cyber and phishing attacks. 2024, 82–86.

[7]. Taherdoost, H. (2024). Insights into cybercrime detection and response: A review of time factor. Information

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

(Basel), 15(5), 273. doi:10.3390/info15050273

[8]. Gupta, P. (2024). Securing tomorrow: The intersection of AI, data, and analytics in fraud prevention. Asian Journal of Research in Computer Science, 17(3), 75–92. doi:10.9734/ajrcos/2024/v17i3425

[9]. Ajala, O. A., Okoye, C. C., Ofodile, O. C., Arinze, C. A., & Daraojimba, O. D. (2024). Review of AI and machine learning applications to predict and Thwart cyber-attacks in real-time. Magna Scientia Advanced Research and Reviews, 10(1), 312–320. doi:10.30574/msarr.2024.10.1.0037

[10]. Publication history: Received on. (2024).

[11]. Puchalski, D., Pawlicki, M., Kozik, R., Renk, R., & Choraś, M. (2024, July 30). Trustworthy AI-based cyber-attack detector for network cyber crime forensics. Proceedings of the 19th International Conference on Availability, Reliability and Security, 1–8. Presented at the ARES 2024: The 19th International Conference on Availability, Reliability and Security, Vienna Austria. doi:10.1145/3664476.3670880

[12]. Chinedu, P. U., Nwankwo, W., Masajuwa, F. U., & Imoisi, S. (2021). Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models. Review of International Geographical Education Online, 11(7).

[13]. Fuad, M. A. F., Rahman, M. H. S., Johara, F. T., Jui, K. F., & Flora, U. M. A. (2023). Trend Analysis and Prediction of Cropped Area of Bangladesh. Asian Journal of Research in Agriculture and Forestry, 9(4), 81-90.

[14]. Milon, M. N. U., Ghose, P., Pinky, T. C., Tabassum, M. N., Hasan, M. N., & Khatun, M. (2024). An in-depth PRISMA based review of cybercrime in a developing economy: Examining sector-wide impacts, legal frameworks, and emerging trends in the digital era. Edelweiss Applied Science and Technology, 8(4), 2072-2093.

[15]. Bacalja, A., Nichols, T. P., Robinson, B., Bhatt, I., Kucharczyk, S., Zomer, C., ... & Schnaider, K. (2024). Postdigital videogames literacies: thinking with, through, and beyond James Gee's learning principles. Postdigital Science and Education, 1-40.

[16]. Monti, M., Stener, M., & Aschi, M. (2022). A computational approach for modeling electronic circular dichroism of solvated chromophores. Journal of Computational Chemistry, 43(30), 2023-2036.

[17]. Alsubaei, F. S., Almazroi, A. A., & Ayub, N. (2024). Enhancing phishing detection: A novel hybrid deep learning framework for cybercrime forensics. IEEE Access

[18]. Balamurugan, M., Dhairiyasamy, R., Bunpheng, W., Kit, C. C., & Gabiriel, D. (2024). Enhanced performance and reduced emissions in LHR engines using Albizia lebbeck antioxidant-infused SBME20 biodiesel. Industrial Crops and Products, 222, 119677

[19]. Djenna, A., Bouridane, A., Rubab, S., & Marou, I. M. (2023). Artificial intelligence-based malware detection, analysis, and mitigation. Symmetry, 15(3), 677

[20]. Kodete, C. S., Thuraka, B., Pasupuleti, V., & Malisetty, S. (2024). Determining the efficacy of machine learning strategies in quelling cyber security threats: Evidence from selected literatures. Asian Journal of Research in Computer Science, 17(8), 24-33