JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation: A Systematic Literature Review

**Vedant Avinash Damedhar[1] , Parag Ravindra Shukla[2] , Prof. Rajat Hedav[3] , Prof. Shubhangi Shinde[4]**

1 , 2 Students , Department of Master of Computer Applications, Dr. D. Y. Patil Centre for Management & Research, Chikhali, Pune, India

3 , 4 Assistant Professor / Associate Professor , Department of Master of Computer Applications, Dr. D. Y. Patil Centre for Management & Research, Chikhali, Pune, India

*Abstract :* This In terms of the current landscape, cybersecurity is a multifaceted and dynamic tapestry that requires comprehensive understanding and vigilance. While AI has the potential to revolutionize cybersecurity, it is also crucial to recognize the potential risks associated with its application. The integration of AI in cybersecurity can provide pivotal benefits, such as enhanced threat detection, proactive security measures, and improved incident response. However, it is worth noting that AI can also be leveraged by cybercriminals to develop more sophisticated and intelligent attacks. As such, it is essential to adopt a strategic and balanced approach to AI adoption in cybersecurity, striking a balance between exploiting its potential benefits and mitigating the associated risks.

*Keywords :* Cybersecurity · Cyber-attacks · DDoS · Man-in-the Middle · Intrusion Detection· Artificial Intelligence.

## I. INTRODUCTION

While the quick adoption of digital technologies in all facets of human life has brought about many benefits, it has also opened the door for more sophisticated cybersecurity risks. The frequency, sophistication, and destructiveness of cyberattacks like ransomware, phishing, data breaches, and denial-of-service (DoS) attacks have increased. When it comes to dealing with dynamic and intelligent threats, traditional cybersecurity defenses—which are frequently static and rule-based—have proven inadequate.

AI is becoming a disruptive force in cybersecurity because of its capacity to learn from data, identify patterns, and adjust to novel circumstances. Businesses can improve their ability to detect, respond to, and prevent threats by integrating AI technologies into their cyber defense systems. In this systematic literature review (SLR), the use of AI to improve cybersecurity is examined. It highlights important AI methods, applications in various cybersecurity domains, difficulties faced, and potential research directions.

## II. LITERATURE REVIEW

The use of artificial intelligence (AI) in cybersecurity has seen significant advancements, helping to address increasingly complex and dynamic security threats in digital environments.

1. **Al-Yaseen et al. (2017)** introduced a multi-level hybrid support vector machine and extreme learning machine, optimized with k-means clustering, for improved intrusion detection, showing the effectiveness of combining traditional and AI-based techniques in identifying diverse attack patterns.

2. **Baptista et al. (2019)** proposed a novel malware detection framework using machine learning and binary visualization methods, demonstrating AI's value in recognizing sophisticated malicious software that evades signature-based tools.

3. **Chowdhury et al. (2018)** and Coull & Gardner (2019) highlighted the role of deep learning and data mining for advanced malware classification, with deep learning models excelling at interpreting complex and adaptive malware behaviors.

4. **Feng et al. (2018)** leveraged neural networks for phishing website detection, while Mahajan & Siddavatam (2018) deployed machine learning algorithms to enhance identification of fraudulent sites, both illustrating the broad applicability of AI in threat detection contexts.

**5. Hashemi et al. (2017)** introduced graph embedding approaches to detect previously unknown malware, underscoring AI's utility for zero-day threat scenarios

## III. Research Questions (RQs)

- RQ1: What are the key AI techniques utilized in the cybersecurity domain ?
- RQ2: How is AI applied to enhance cybersecurity measures in various areas ?
- RQ3: What challenges and limitations are associated with integrating AI into cybersecurity ?
- RQ4: What future research directions and improvements can enhance the effectiveness of AI in cybersecurity ?

## IV. Methodology

### 4.1 Data Sources

A variety of academic databases and digital libraries were searched in order to perform this review, including :

- IEEE Xplore
- SpringerLink
- ACM Digital Library
- Elsevier ScienceDirect
- Google Scholar

### 4.2 Search Strategy

"AI in cybersecurity," "deep learning network security," "machine learning cyber defense," "AI intrusion detection," and "cyber threat mitigation with AI" were among the search terms used. To refine the search and combine terms, boolean operators were employed.

### 4.3. Inclusion and Exclusion Criteria

**Inclusion Criteria :**

- Articles published between 2016 and 2022
- Peer-reviewed publications
- English language
- Focused on AI-based cybersecurity applications

**Exclusion Criteria :**

- Non-peer-reviewed content
- Non-English language
- Studies focusing solely on traditional (non-AI) cybersecurity methods

### 4.4. Data Extraction and Synthesis

A standardized form was used to extract data that included the study's goals, AI methods employed, application domain, results, and limitations. The results were compared and analyzed using a narrative synthesis approach.

---

## V. AI Techniques in Cybersecurity (RQ1)

Artificial Intelligence (AI) includes a variety of methods that have been successfully used in cybersecurity.

### 5.1 Machine Learning (ML)

Without explicit programming, ML allows systems to learn from data and enhance performance. Learning under supervision (e.g. G. SVM, decision trees) is frequently employed in the detection of spam and phishing, whereas unsupervised learning (e.g. G. clustering) is employed to identify anomalies.

### 5.2 Deep Learning (DL)

As a subset of machine learning, deep learning (DL) models intricate patterns using multi-layer neural networks. In traffic analysis, behavior prediction, and malware classification, it has demonstrated remarkable success.

### 5.3 Natural Language Processing (NLP)

NLP is used to analyze data related to human language. Through text processing and interpretation, it is used in cybersecurity to identify malicious content, phony URLs, and phishing emails.

### 5.4 Expert Systems

These systems replicate human decision-making through the application of a set of rules to a knowledge base. They are employed in intrusion detection systems (IDS) to appraise threats based on predefined rules and expert knowledge.

### 5.5 Reinforcement Learning (RL)

In the context of cybersecurity, Reinforcement Learning is being utilized as a tool to automate threat response and mimic the behavior of an attacker. This learning process involves agents discovering the most effective actions through a series of trials and errors. This approach is of pivotal importance due to the complex and multifaceted nature of the cybersecurity landscape.

## VI. Applications of AI in Cybersecurity (RQ2)

The integration of Artificial Intelligence (AI) is increasingly prevalent within the cybersecurity domain, serving to augment threat identification, reaction, and mitigation

### 6.1 Intrusion Detection Systems (IDS)

By enhancing the ability to identify anomalous activity in network traffic, AI improves IDS.
High accuracy detection of possible intrusions is achieved through the use of machine learning algorithms like SVM, k-means clustering, and neural networks.

### 6.2 Malware Detection

By learning from previously seen malware samples, AI-based systems are able to identify malware variants. To identify possible dangers, these systems examine source code, binary files, and behavioral patterns.

### 6.3 Phishing and Spam Detection

Phishing attempts are identified in emails and websites using NLP and ML models. These systems search for suspicious links, sender information, and linguistic patterns.

### 6.4 Behavioral Analysis

Through user behavior monitoring, AI spots irregularities that could point to compromised accounts or insider threats. For ongoing authentication, behavioral biometrics can be employed.

### 6.5 Risk Assessment and Management

AI models can forecast possible weaknesses by examining threat intelligence feeds, system configurations, and historical data. Thus, proactive risk mitigation is made possible.

### 6.6 Fraud Detection

AI is used in banking and e-commerce to identify anomalous patterns in transaction histories and user behavior, which helps identify fraudulent transactions.

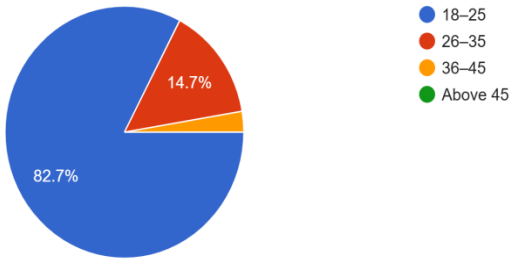
## VII. Data Ananysis and Interpretation

1) Age

| Options | Respondents | Percentage |
|---|---|---|
| Below 18 | 2 | 3.2% |
| 18 – 26 years | 59 | 93.7% |
| 26-30 years | 1 | 1.6% |
| Above 30 | 1 | 1.6% |
| **Total** | **63** | **100%** |

Table 1: Table shows respondent age

The table shows that most respondents (93.7%) are aged 18–26 years, indicating a predominantly young participant group. The pie chart visually confirms this distribution, with the 18–26 age group forming the largest segment of the sample



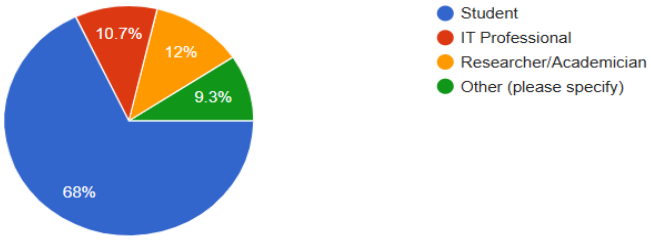

Graph 1: Graph shows respondent age

2) Current Role/Occupation

| Options | Respondents | Percentage |
|---|---|---|
| Student | 51 | 68% |
| IT Professional | 8 | 10.7% |
| Researcher/Academician | 9 | 12% |
| Other(Other specify) | 7 | 9.3% |
| **Total** | **75** | **100%** |

Table 2: Table shows Current Role Distribution

The data shows that most respondents (68%) are students, followed by researchers/academicians (12%) and IT professionals (10.7%). This indicates the majority of participants are from academic backgrounds, with fewer professionals represented



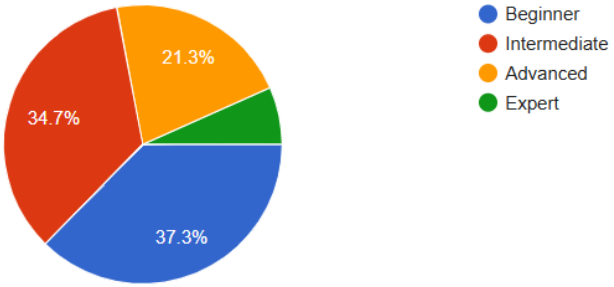

Graph 2: Graph shows respondent current role/occupation

3) How would you rate your knowledge of cybersecurity?

| Options | Respondents | Percentage |
|---|---|---|
| Beginer | 28 | 37.3% |
| Intermediatel | 26 | 34.7% |
| Advanced | 16 | 21.3% |
| Expert | 5 | 6.7% |
| **Total** | **75** | **100%** |

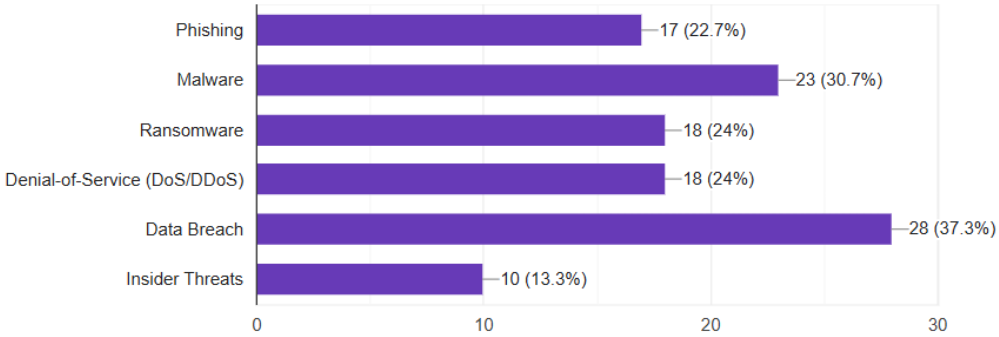
Table 3: Table shows Cybersecurity Knowledge Ratings

The table shows that 37.3% of respondents consider themselves beginners in cybersecurity, with only 6.7% viewing themselves as experts. This suggests that the overall cybersecurity knowledge among participants is more basic than advanced.




Graph 3: Graph shows Distribution of Cybersecurity Knowledge

4) Which of the following cyber threats are you most concerned about?




Graph 4: The graph shows the respondents Cyber Threat Concerns

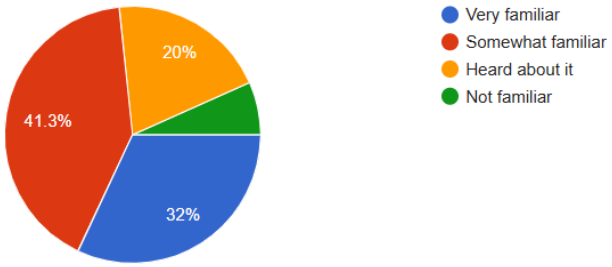
The chart shows that data breaches are the top concern among respondents (37.3%), followed by malware and ransomware threats. Phishing and insider threats are relatively less worrisome for the surveyed group.

5) How familiar are you with Artificial Intelligence applications in cybersecurity?

| Options | Respondents | Percentage |
|---|---|---|
| Very familiar | 24 | 32% |
| Somewhat familiar | 31 | 41.3% |
| Heard about it | 20 | 20% |
| Not familiar | 5 | 6.7% |
| **Total** | **75** | **100%** |

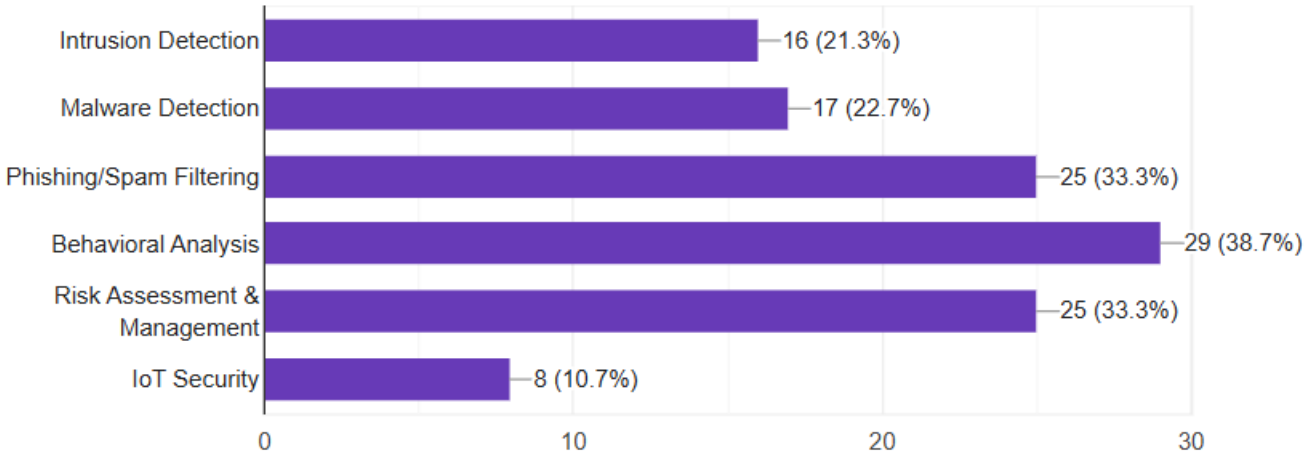
Table 5: Table shows AI Familiarity in Cybersecurity

Most respondents are at least somewhat familiar with AI applications in cybersecurity, with 41.3% being somewhat familiar and 32% very familiar. Only a small portion (6.7%) are not familiar with these AI concepts.




Graph 5: AI Familiarity Graph

6) In your opinion, where can AI be most useful in cybersecurity?




Graph 6: Graph shows AI Use Cases in Cybersecurity

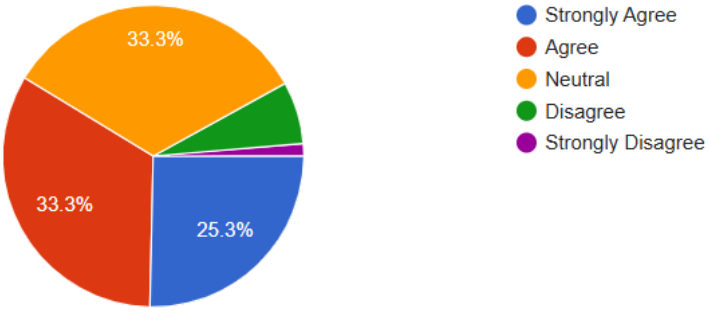
Behavioral analysis is seen as the most valuable AI use case in cybersecurity (38.7%), followed by phishing/spam filtering and risk assessment. IoT security is the least chosen area for AI application among respondents.

7) Do you agree that AI provides better cybersecurity compared to traditional methods?

| Options | Respondents | Percentage |
|---|---|---|
| Strongly Agree | 19 | 25.3% |
| Agree | 25 | 33.3% |
| Neutral | 25 | 33.3% |
| Disagree | 5 | 6.7% |
| Strongly Disagree | 1 | 1.3 |
| **Total** | **75** | **100%** |

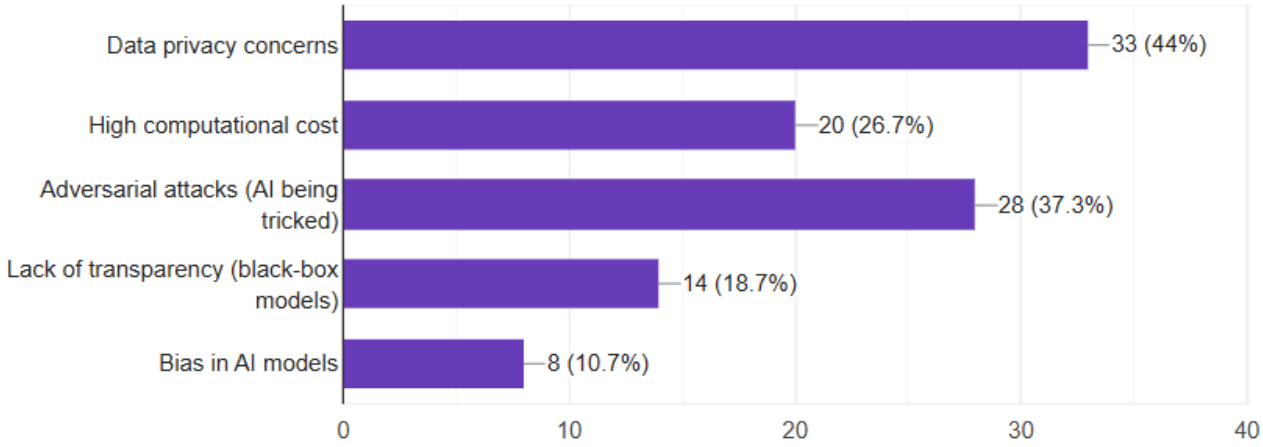
Table 7: AI vs Traditional Cybersecurity Opinions

Most respondents either agree (33.3%) or strongly agree (25.3%) that AI provides better cybersecurity than traditional methods, while only a small segment disagrees. A significant portion (33.3%) remains neutral on this topic.




Graph 7: AI Effectiveness Opinion Graph

8) What challenges do you see in adopting AI for cybersecurity?




Graph 8: Graph shows Challenges in Using AI for Cybersecurity

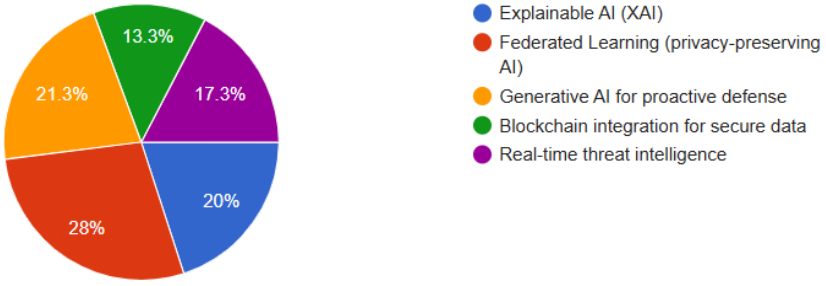
Data privacy concerns are the most cited challenge in adopting AI for cybersecurity (44%), followed by the risk of adversarial attacks and high computational costs. Issues of transparency and model bias are less frequently mentioned by respondents.

9) What should be the top priority for future AI in cybersecurity?

| Priority | Level | Percentage |
|---|---|---|
| Explainable AI (XAI) | 15 | 20% |
| Federated Learning | 21 | 28% |
| Generative AI for proactive defense | 16 | 21.3% |
| Blockchain integration for secure data | 10 | 13.3% |
| Real-time threat intelligence | 13 | 17.3% |
| **Total** | **75** | **100%** |

Table 9:Table shows future AI Priorities in Cybersecurity

Federated learning is the most preferred priority for future AI in cybersecurity (28%), followed by generative AI for proactive defense and explainable AI. Blockchain integration and real-time threat intelligence are viewed as less urgent by respondents.



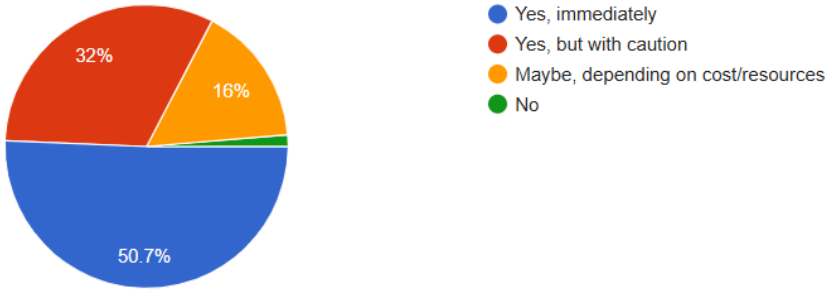

Graph 9: Graph shows AI Priority Distribution

10) Would you recommend organizations to adopt AI-driven cybersecurity systems?

| Options | Respondents | Percentage |
|---|---|---|
| Explainable AI (XAI) | 38 | 50.7% |
| Federated Learning | 24 | 32% |
| Generative AI for proactive defense | 12 | 16% |
| Blockchain integration for secure data | 1 | 1.3% |
| **Total** | **75** | **100%** |

Table 10: Table shows AI Adoption Recommendation

Over half the respondents (50.7%) recommend organizations adopt explainable AI for cybersecurity, while 32% suggest federated learning as the next best option. Generative AI and blockchain integration are far less prioritized among recommendations.




Graph 10: AI Cybersecurity Adoption Graph

## VIII. Challenges and Limitations (RQ3)

Despite the benefits, the integration of AI in cybersecurity is not without challenges:

- Data Requirements: Large volumes of labeled data are needed for training AI models, but obtaining this data may be challenging because of privacy or availability issues.
- Adversarial Attacks: These attacks involve creating adversarial examples, or inputs, that trick AI models.
- Model Interpretability: A large number of AI models, particularly deep learning models, are "black boxes" with opaque decision-making processes.
- The deployment and training of AI models necessitate a substantial amount of infrastructure and processing power.
- Fairness and Bias: AI models may generate unfair or erroneous results if training data is biased.

## IX. Comparison of AI Techniques

| Technique | Pros | Cons |
|---|---|---|
| Machine Learning | Interpretable, fast training | Requires labeled data |
| Deep Learning | High accuracy, handles complex data | High resource consumption |
| NLP | Effective for text analysis | May misread context |
| Expert Systems | Rule-driven and explainable | Inflexible and hard to scale |
| Reinforcement Learning | Adaptive and self-improving | Complex and time-consuming to train |

## X. Future Directions (RQ4)

### 10.1 Explainable AI (XAI)

Building AI models that can describe how they make decisions will improve human oversight and foster greater trust.

### 10.2 Federated Learning

This privacy-preserving method improves data security and compliance by enabling AI models to be trained on dispersed data sources without centralizing data.

### 10.3 Blockchain Integration

Blockchain technology and artificial intelligence (AI) can improve the security and integrity of data used for inference and training.

### 10.4 Real-time Threat Intelligence

Preventing breaches requires the development of low-latency AI systems that can evaluate streaming data and issue real-time alerts.

### 10.5 IoT Security

Lightweight AI models are required as IoT devices proliferate in order to identify threats on devices with limited resources.

.

## XI. Conclusion

Artificial intelligence is transforming cybersecurity by providing scalable, intelligent, and adaptive threat detection and mitigation solutions. Even though AI has many advantages over conventional systems, there are a number of issues with data, transparency, and adversarial robustness that must be resolved before it can be put into practice. With more study and development, AI has the potential to greatly improve cybersecurity resilience worldwide.

## XII. References


1. Al-Yaseen, W., Othman, Z., Ahmad Nazri, M.Z. (2017). Multi-level hybrid support vector machine and extreme learning machine based on modified k-means for intrusion detection system. *Expert Systems with Applications*, 67.
2. Baptista, I., Shiaeles, S., Kolokotronis, N. (2019). A novel malware detection system based on machine learning and binary visualization. *IEEE ICCW*.
3. Chowdhury, M., Rahman, A., Islam, M.R. (2018). Malware analysis and detection using data mining and machine learning classification. *Springer*, pp. 266–274.
4. Coull, S., Gardner, C. (2019). Activation analysis of a byte-based deep neural network for malware classification. *IEEE SPW*, pp. 21–27.
5. Demetrio, L., Biggio, B., Lagorio, G., Roli, F., Armando, A. (2019). Explaining vulnerabilities of deep learning to adversarial malware binaries.
6. Feng, F. et al. (2018). The application of a novel neural network in the detection of phishing websites. *Journal of Ambient Intelligence and Humanized Computing*.
7. Feng, W. et al. (2016). A support vector machine based naive Bayes algorithm for spam filtering.
8. Hashemi, H. et al. (2017). Graph embedding as a new approach for unknown malware detection. *Journal of Computer Virology and Hacking Techniques*, 13.
9. Mahajan, R., Siddavatam, I. (2018). Phishing website detection using machine learning algorithms. *IJCA*, 181.
10. Ye, Y. et al. (2018). DeepAM: a heterogeneous deep learning framework for intelligent malware detection. *Knowledge and Information Systems*, 54.
11. Cybersecurity Ventures. (2022). Annual Cybercrime Report.
12. World Economic Forum. (2022). Global Cybersecurity Outlook 2022.