International Journal of Computers and Informatics (IJCI)
Vol. (5), No. (2)
IJCI
February 2026
المجلة الدولية للحاسبات والمعلوماتية
الإصدار (5)، العدد (2)

A Comparative Study of Artificial Neural Networks and Reinforcement Learning Models

Sabah Abdellatif Hassan Ahmed
Assistant Professor, Faculty of Information Technology, University of Bisha, Kingdom of Saudi Arabia
sahmad@ub.edu.sa

Abstract

Cyber-attacks have grown more sophisticated, posing critical threats to national infrastructure and data integrity. Deep learning methods, particularly Artificial Neural Networks (ANNs) and Reinforcement Learning (RL), offer promising capabilities in cyber threat detection and response. However, existing approaches face limitations in scalability, data sufficiency, and real-time adaptability. This study conducts a comparative analysis of ANNs and RL models to assess their effectiveness in analyzing cyber-attacks within the Saudi National Cybersecurity Authority. Using a descriptive analytical approach, data were gathered from 105 experts via questionnaires and 10 specialists through interviews. Results reveal that both models exhibit high performance in detection accuracy, adaptability, and operational efficiency. Nevertheless, challenges persist, including data dependency and interpretability. The study contributes by (1) evaluating the current implementation of ANNs and RL in Saudi cybersecurity infrastructure, (2) identifying practical and technical limitations of each model, and (3) recommending adaptive, hybrid strategies for enhanced cyber defense using deep learning.

Keywords: Cyber-Attack, Deep Learning, Artificial Neural Networks, Reinforcement Learning Models.

Introduction

Network cyberattacks are getting more intricate and sophisticated every day. It is now difficult for organizations to protect their digital assets. Keeping computer systems and networks safe from cyberattacks of any kind is crucial. These attacks must be detected, which is a crucial component of any security tool, to be prevented (Gjylapi

et al.). As a result, cybersecurity has become a priority for the national security of different nations. The goal of cybersecurity, a specialized field of information technology, is to protect information assets' availability, confidentiality, and integrity. This is an important turning point in human technological development, and it tends to develop with new methods and practices that offer secure ecosystems (Hernandez-Suarez et al., 2023; Podder et al., 2021). Traditional deep packet inspection and intrusion detection methods, though still in use, are not effective enough to meet the changing security threats (Delplace et al., 2020).

While Artificial Intelligence (AI) is currently employed in many fields, its revolutionary influence on cybersecurity is unparalleled. AI has been seen as a major component of cybersecurity, bringing with it automation of responses, network threat detection, and security consciousness (Muheidat et al., 2024). Business environments and government entities have begun automating the intricate procedures for identifying attacks and responding to breaches through the use of AI. From the standpoint of incident response, AI is especially potent since it can identify patterns and anomalies much more accurately than any human agent could. Through “AI, machine learning (ML), and deep learning (DL) technologies”, analysts can now react to threats more quickly and confidently. Strategic companies and enterprises will be able to stay ahead of the curve thanks to AI automated cyber security incident response (CYBERSECURITY).

ML and DL are tools that cybersecurity professionals can use to help make systems safer. In cybersecurity, network attacks can be tracked and avoided using “machine learning and DL classification algorithms”. It is used to spot system anomalies that might indicate an active attack (Ghazal & Mjlae, 2022; Okafor, 2024). Thus, “ML and DL based cybersecurity applications” offer critical ways to identify “malware and zero-day attacks” (Podder et al., 2021). The current investigation delves deeper into the capacity DL algorithms (Artificial Neural Networks and Reinforcement Learning) to bolster cybersecurity defenses against dynamic threats. Crucially, these algorithms

offer adaptive, real-time threat detection, consequently shortening the response time to cyber incidents.

Problem Statement

Despite of numerous approaches to intrusion detection, forecasting future cyberthreats is still a research challenge (Samia, 2023). The use of ML and DL techniques in "intrusion detection systems" has shown promise in effectively identifying network intrusions (Azam, Islam & Huda, 2023). The problem lies in "the lack of sufficient data to utilize ML and DL algorithms" to automate human intelligence (CYBERSECURITY). While prior reviews showed, to some extent, how machine learning (ML) applications were deployed in different cyberspace domains, less emphasis has been paid to the role of DL techniques in this regard (Aaron, 2023). At the Saudi level, ICT has evolved into a fertile environment for various types of cybercrimes such as deceit, blackmail, online frauds, financial frauds, cyberbullying, and more (Alzhrani et al.).

Harnessing AI technology for the detection, surveillance, and analysis of transactions to ensure the safety of capital and private information has become a priority for the Saudi Government. Deploying AI and machine learning systems to secure cloud environments against the most prevalent means of malware intrusion is of utmost importance (*Fintech Saudi Deep Dives: Cybersecurity Solution Opportunities in KSA. Deloitte & Touche*, 2021). Based on above statement, an efficient choice for improving cyber threat detection and response is AI, specifically DL algorithms. However, there is enough comparative research on how well various AI models fight with cyberattacks more especially Reinforcement Learning (RL) and Artificial Neural Networks (ANNs). These models' performance, adaptability, and practical application within Saudi Arabia's cybersecurity infrastructure are still poorly understood, despite their demonstrated promise in cybersecurity applications.

Research Questions

1. What is the reality of using artificial neural networks in analysing cyber-attacks in the Saudi National Cybersecurity Authority?
2. What is the reality of using reinforcement learning models in analysing cyber-attacks in the Saudi National Cybersecurity Authority?

Research Objectives

1. Determine the reality of using artificial neural networks in analysing cyber-attacks in the Saudi National Cybersecurity Authority.
2. Define the reality of using reinforcement learning models in analysing cyber-attacks in the Saudi National Cybersecurity Authority.

Research Significance

The Kingdom prioritizes cybersecurity and digital transformation in its Vision 2030. Growing cyberthreats have targeted Saudi Arabia, especially its critical infrastructure. It is difficult for traditional cybersecurity systems to identify zero-day attacks and advanced persistent threats. ANNs and Reinforcement Learning, two DL algorithms, can strengthen cybersecurity defenses against changing threats, according to the study. The study assists in determining the best strategy for threat detection and prevention by examining and contrasting these models. This study has wide-ranging effects on Saudi Arabia's digital transformation, national security, adoption of AI, and cybersecurity strategy. It will provide all information for promoting public and private sectors' cyber defenses. The results will help inform future AI research, cybersecurity professionals, industry practitioners, and policy decision-makers.

Literature Review

AI in Cybersecurity:

The rules, techniques, and instruments that work together to protect networks, software, data, and computer resources from attacks on their confidentiality and integrity are collectively referred to as cybersecurity. To prevent attacks and find

security flaws, "firewalls, antivirus software, intrusion detection systems, and intrusion protection systems" are essential tools (Berman et al., 2019; Podder et al., 2021). The growth of internet technology and the rise in participation in online communities have made networks more susceptible to cyberattacks, which can seriously harm people and organizations by resulting in identity theft, financial loss, and reputational damage. Conventional methods, such as “rule-based firewalls & signature-based detection”, often struggle to effectively combat increasingly dynamic and complex cyberthreats (Oh et al., 2023). To predict and detect crime, cyber-attack analysis is needed (Samia, 2023). Many researchers confirm that AI, ML, and DL are effective tools in cyberattack analysis (Ghazal & Mjlae, 2022; Sarker, 2021). These interrelationships are represented in Figure (1).

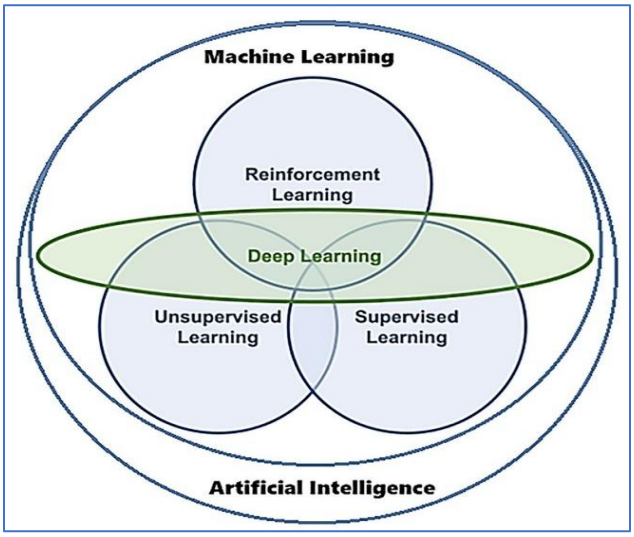


Figure (1): Interrelationships among variables taken from (Al-Nawashi et al., 2025)

However, three paradigms are used in machine learning to describe how computer programs learn to generate results from experiments: “supervised, unsupervised, and RL”. On one hand, supervised learning is an algorithm where “labels from the input data are used to train the model”. On the other hand, unsupervised learning is “patterns found in the input data are used to train the model”. Reinforcement Learning (RL) represents “a software agent learns to respond autonomously to an environment that

it is not yet familiar with" (KABANDA et al., 2023). Figure (2) represents that ML algorithm that are commonly used for cyber security.

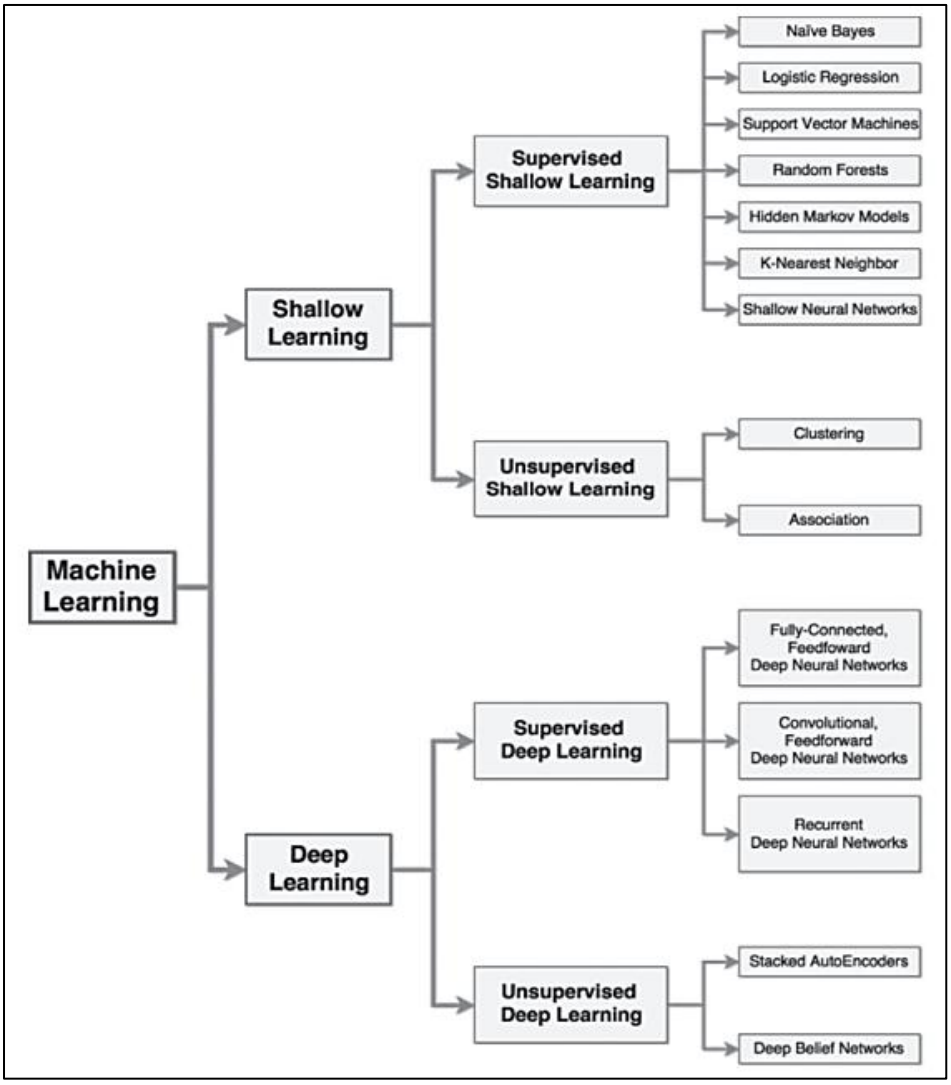


Figure (2): ML algorithm in cyber security extracted from (Apruzzese et al., 2018)

Developers often mix up labels like ML and DL, treating them as if they're one and the same. In truth, each term points to a machine that's been programed to pick up clues and decide the best way to fix a problem. Generally speaking, ML falls under the broad umbrella of artificial intelligence, while DL is really just a part of the machine learning world. When building an effective "intrusion detection system",

programmers usually depend on both approaches, blending their strengths in ways that maximize their expected results (Halbouni et al., 2022; Xin et al., 2018).

It was initially suggested that DL would improve the efficiency of neural networks and the accuracy of output predictions by increasing the number of intermediate {Mienye, 2024 #4}. Neural networks can handle complex unstructured data types such as malware samples and network traffic, giving them an advantage over traditional ML techniques in terms of "detection accuracy" and "fewer false positives". DL models can also comprehend "subtle irregular patterns" that imply cyber threats (Li et al., 2021; Muheidat et al., 2024).

When it came to identifying and classifying cyberattacks, (Bapiyev et al., 2017) have confirmed that the DL model demonstrated exceptional accuracy. It proved to be resilient in recognizing "malware injections and DDoS attacks". Both the recall and precision scores were continuously high. Furthermore, DL techniques present a crucial chance to spot new malware variations and zero-day attacks. These attacks primarily target data, host systems, targeted networks, and application software (Podder et al., 2021).

Artificial Neural Networks (ANNs):

DL methods are based on "neural networks" or "artificially generated neural networks". Their shape and name are modeled after the human brain, and they mimic the communication between actual neurons. The massively parallel systems known as ANNs are made up of a vast number of interconnected basic processor (Qamar & Zardari, 2023). Neural networks are computer models that can process data to solve problems like regression and classification. This aspect of AI draws inspiration from the human nervous system and brain) Tian et al., 2022(ANNs are DL algorithms with nodes that mimic cell body behavior and are connected by axons and dendrites (Samia, 2023).

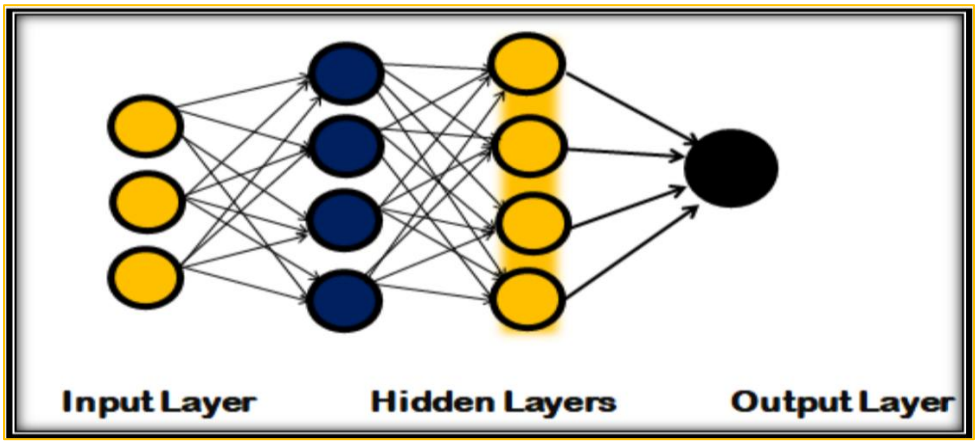
The network can be any number of cells, nodes, units, or neurons. It connects the input set and the output. It is a piece of software that mimics how the human brain processes

information and makes decisions. Neural networks are gaining popularity lately because of their remarkable performance when there is a lot of data available (Delplace et al., 2020). One can identify various DL techniques used in cyber security as follows:

- **"Deep Belief Networks - DBNs":** In a groundbreaking work, Geoffrey Hinton introduces DBNs. A subclass of Deep Neural Networks (DNNs) are DBNs. There are multiple layers of hidden causal variables that make up a DBN. Additionally, each layer has connections between its units, but not between the layers. It is the integration of ML and neural networks with probability and statistics.
- **"Autoencoder"**: In an unsupervised approach, an autoencoder uses a vector as input. The network endeavors to link the input with the output, which is the same as the input vector. By adjusting the input and re-creating it in a different dimensionality, a visualization of the data can be created with either fewer or more dimensions. This process of data representation, referred to as data encoding or feature compression, takes place within the network using layers that have compact dimensions.
- **"Recurrent Neural Networks - RNNs":** RNNs are the best tool for processing sequential data, where the details of the data elements' order and context are crucial. RNNs remember and make use of information from earlier steps or time points in the sequence, whereas feedforward neural networks process data in a single pass from input to output. The RNN, or recurrent layer, is composed of recurrent units, or cells. Within every cell is a state called "memory" that is updated continuously and carried over to the subsequent step of the sequence. By serving as a context, this memory allows the network to recognize dependencies and patterns that persist across a variety of time steps.
- **"Convolutional Neural Network – CNN**": It examines input from visual imagery. A grayscale or colored image will be saved in pixels, much like a 2D array, if it is entered. Moreover, CNNs are employed to control audio spectrograms with 2D arrays.

- **"Generative Adversarial Networks – GANs":** Two neural networks compete to outperform one another in a zero-sum game that is used in unsupervised machine learning.
- **"Recursive Neural Network":** In recursive neural networks, a series of weights are linked in a recursive fashion. These networks accept multiple inputs, with the key two inputs initially combined as a single element in the model. Afterwards, a node's output functions as the input for the subsequent node. Multiple models of this nature are leveraged for tasks like image segmentation and natural language processing.
- **"Deep Reinforcement Learning – DRL**": Making AI agents that are human-like or even superhuman has emerged as one of the most effective strategies. When DNNs and a traditional RL framework are combined to handle complex and high-dimensional sequential decision-making problems, this accomplishment is frequently the outcome. Consequently, DRL algorithms have been applied in cybersecurity and the Internet of Things (IoT), among other fields (Azam et al., 2023; Berman et al., 2019; Dahl et al., 2013; Delplace et al., 2020; Goodfellow et al., 2014; Hihi & Bengio, 1995; Nguyen & Reddi, 2021; Podder et al., 2021).

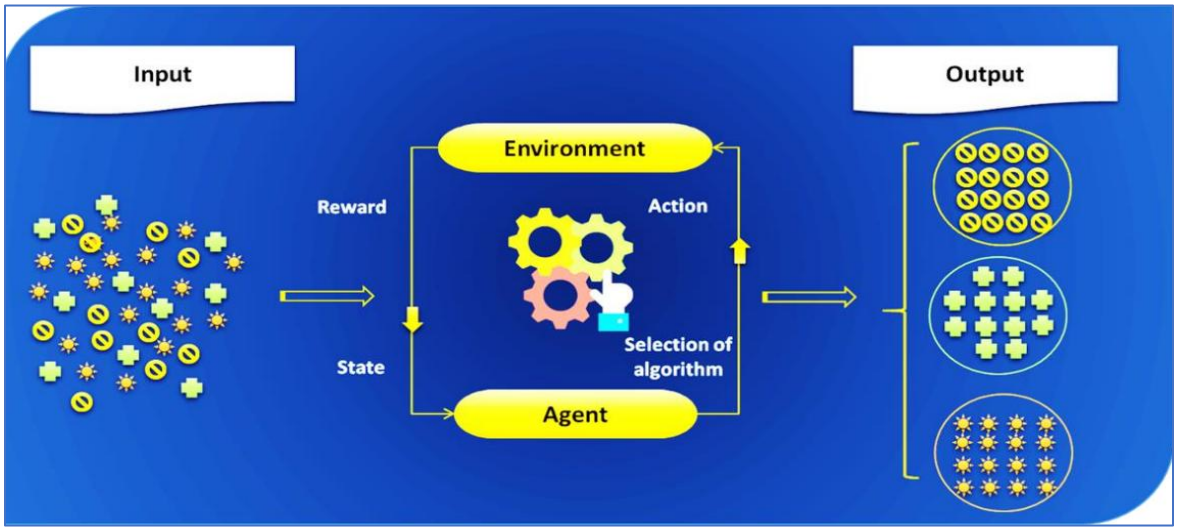
The "neural network" consists of three layers of subunits. The "input layer" of a neural network consists of "artificial input neurons". They send information for processing to the system from the initial layers of neurons. The workflow is started by the neural network's input layer. The number of inputs determines the weights of the input and output of the artificial neurons in the hidden layer, which reflects input and output layers. Before reaching the output, data must first arrive at the data sources and then proceed layer by layer through the network (Qamar & Zardari, 2023). The layers of these ANNs are represented in Figure (3).



Figure(3): Artificial Neural Networks extracted from (Qamar & Zardari, 2023)

Reinforcement Learning (RL):

This method of learning optimizes an agent's actions in a probabilistic environment by using trial and error. The environment provides the agent with a response and a reward after the agent acts at each time step (Mousavi et al., 2018; Thomas et al., 2019). The RL components are "policy, reward signal, value function and an optional environment management model that controls what happens next" (KABANDA et al., 2023). The components of RL are represented in Figure (4).



Figure(4): Reinforcement Learning Components extracted from (Abouhawwash, 2024)

The explanation of RL major elements can be provided as follows:

1. **Agent:** The person who deals with the environment.
2. **Environment:** everything that the agent encounters and absorbs knowledge from. The "agent" obtains feedback, new states and rewards, from "the environment".
3. **Policy:** It is essentially a set of instructions that connect the detected environmental conditions to the actions to be taken when those states are present.
4. **Reward signal:** The reward indicator signifies the goal. The environment provides a solitary numerical value, referred to as the reward, to the RL agent at each moment in time. The objective of the agent is to optimize its cumulative reward over a prolonged period. Alterations to the policy are executed based on the reward signal.
5. **Value**: Value evaluations serve as the foundation for decisions about what to do. Behaviors that produce the highest value states are preferred over those that aim for the biggest reward. The set of observations an agent makes during its lifetime must be used to update values on a regular basis (Abouhawwash, 2024; KABANDA et al., 2023; Oh et al., 2023).

Different categories of "RL algorithms" are Monte Carlo, "SARSA: State-action-reward-state-action", "DQN: Deep Q network", "SARSA-Lambda: State-action-reward-state-action with eligibility traces", "DDPG: Deep deterministic policy gradient", "A3C: Asynchronous actor-critic algorithm", "NAF: Q-Learning with normalized advantage functions", "PPO: Proximal policy optimization", "TRPO: Trust region policy optimization" (Thomas et al., 2019). The impact of "RL" research on the defense of distributed cyber-physical systems has been substantial. Given that AI can push the security level of these systems to a peak level, its role in "cybersecurity" is indispensable (KABANDA et al., 2023). RL has demonstrated significant promise in addressing intricate decision-making issues across a range of fields, including cybersecurity (Oh et al., 2023). Cybersecurity issues can be addressed with RL, which enables "defense mechanisms" to adjust to evolving threats (Safeer, 2025).

Research Procedures

Research Methodology:

The study adopted the descriptive analytical method defined by {Aldosari, 2020 #4} as "one of the forms of organized scientific analysis and interpretation used to describe a specific phenomenon or problem, and measure it by collecting standard data and information about the phenomenon or problem, classifying and analyzing it, and then carefully examining it."

Population & Sample:

The study population contained all cybersecurity experts in the Saudi National Cybersecurity Authority. A sample random sampling technique was utilized. The study engaged 105 experts for the questionnaire tool and an additional 10 specialists for in-depth interviews, ensuring a diverse and representative insight from the target population.

Research Sample Characteristics:

The study sample's general information was analyzed, focusing on key demographic factors such as gender and years of experience, as outlined below:

Table (1): Research Sample Characteristics

Gender	Frequencies	Percentages
Male	77	73.3%
Female	28	26.7%
Total	105	100%
Years of experience	Frequencies	Percentages
Less than 5 years	19	18.1%
From 5 to 10 years	37	35.2%
More than 10 years	49	46.7%
Total	105	100%

The sample majority, representing (73.3%) are (male), while females account for the remaining (26.7%) in terms of years of experience the largest proportion (46.7%) have more than 10 years of experience, followed by (35.2%) with experience ranging from

(5 to less than 10 years), and the smallest group (18.1%) with (less than 5 years of experience).

Study Tools (Questionnaire, Interview):

The "researcher" reviewed the study objectives that aimed to reveal the analysis of cyber-attacks using DL algorithms through a comparative study of ANNs and RL models. After reviewing the theoretical literature and previous studies related to the research topic, it was found that the most appropriate means of collecting data is (the questionnaire), which (Al-Dhamen, 2007) defined as "a means of collecting information, and it may be used in a broad framework to include the nation or in a narrow framework on the scale of the school, and of course it differs in its length and degree of complexity, in addition to the fact that the greatest effort in the questionnaire is focused on building good statements and obtaining complete responses, and it is very important that the research questions and hypotheses are clear and known so that it is possible to build the paragraphs well."

Drawing on theoretical literature and previous studies, the researcher structured the questionnaire by defining its key axes and dimensions. Each axis was carefully outlined, with corresponding statements formulated to align with the study's objectives. The final questionnaire was structured as follows:

The Description of the study tool (Questionnaire):

The final version of the questionnaire consists of two main parts:

The first part contains preliminary data on the study sample, focusing on demographic information such as gender and number of years of experience.

The second part comprises the main questionnaire components, structured into two key axes, outlined as follows:

- The first axis: Using ANNs in analysing cyber-attacks, and includes statement No. (1) to statement No. (10).

- The second axis: Using RL models in analyzing cyber-attacks, and includes statement No. (11) to statement No. (20).

The five-point Likert scale (strongly agree, agree, Neutral, disagree, strongly disagree) was used to correct the research tool, giving the response: strongly disagree (1), disagree (2), neutral (3), agree (4), strongly agree (5).

The validity and reliability of the tool (Questionnaire):

1. **Arbitrators Validity (Questionnaire):** After creating the questionnaire and formulating its statements, a group of subject-matter experts evaluated it to determine how well it met the goals of the research. The evaluation aimed to ensure the relevance of each statement to its respective axis, the clarity of wording, the linguistic accuracy, and the overall alignment with the intended purpose. The experts also provided recommendations for improvement, including modifications such as deletion, addition, or rewording, as deemed necessary.

   After retrieving the arbitrators' peer-reviewed copies, the researcher revised the questionnaire based on their suggestions. Some statements were removed and reworded, as approved by over 80% of the honorable arbitrators. As a result, the questionnaire took on its final form after its face validity was confirmed, with 20 statements spread across two axes.

2. **Validity of the tool (Questionnaire):** The validity of the tool refers to its ability to accurately measure what it was designed to assess. The validity of the (questionnaire) was determined as follows:

   The internal consistency validity was assessed by calculating the Pearson correlation coefficient between each statement's score and the total score of its corresponding axis in the questionnaire, as illustrated in Table (2).

Table (2): Pearson correlation coefficients between the scores of each statement and the total score of the axis to which the statement belongs in the questionnaire

Statement No.	Correlation coefficient	Statement No.	Correlation coefficient	Statement No.	Correlation coefficient
First axis: Using artificial neural networks in analyzing cyber-attacks					
1	.771**	2	.729**	3	.757**
4	.726**	5	.839**	6	.758**
7	.793**	8	.723**	9	.739**
10	.848**				
Second axis: Using reinforcement learning models in analyzing cyber-attacks					
11	.789**	12	.708**	13	.777**
14	.721**	15	.761**	16	.788**
17	.802**	18	.778**	19	.716**
20	.770**				

"**Statistically significant at the (0.01) significance level"

The table above shows that the Pearson correlation coefficients of the statements with the total score of the axis to which the statement belongs in the questionnaire were all statistically significant at the (0.01) significance level, and all of the values of the correlation coefficients were significant, as they ranged in the first Using ANNs in evaluating cyber-attacks between (723** -.848**), and ranged on the second axis: Using RL models in analyzing cyber-attacks between (.708**-.802**), confirming a good level of internal consistency validity for the statements within the questionnaire axes.

The construct validity of the questionnaire axes was confirmed by calculating the correlation coefficients between the total score of each axis and the overall questionnaire average, the results are presented in Table (3).

Table (3): Correlation coefficients between the total score of each axis and the overall questionnaire average

No.	Axes	Correlation coefficient
1	First axis: Using artificial neural networks in analyzing cyber-attacks	.882**
2	Second axis: Using reinforcement learning models in analyzing cyber-attacks	.867**

"**Statistically significant at the (0.01) significance level"

The table above demonstrates that the correlation coefficients values for the questionnaire axes are high, ranging between (.867**- .882**), with all values

being statistically significant at the (0.01) level; this confirms a strong degree of construct validity for the questionnaire.

3. **Tool Reliability (Questionnaire):** Reliability of the tool means ensuring that the answer will be approximately the same if it is applied repeatedly to the same people at different times, and the reliability of the tool (questionnaire). The questionnaire reliability was estimated using "Cronbach's Alpha method" as follows:

Table (4): Cronbach's Alpha reliability coefficients for the questionnaire axes

No.	Axes	Cronbach's Alpha
1	First axis: Using artificial neural networks in analyzing cyber-attacks	.923
2	Second axis: Using reinforcement learning models in analyzing cyber-attacks	.919
Overall reliability coefficients		.935

Table (4) demonstrate that the values of the reliability coefficients for the questionnaire axes came in high values, ranging between (.919- .923), and the value of the total stability coefficient reached (.935); these values confirm the suitability of the questionnaire axes for application and ensure the credibility and dependability of the results.

4. **Description of the research tool (interview):** Since the current research method is qualitative, the researcher has previously prepared a set of open questions that would help achieve the main objective of the research. All interview questions are (Open-ended questions) and a (Semi-structured) model was adopted. This model depends on adhering to the pre-determined interview questions with the addition of other questions that may appear during the interview. The open questions that were prepared in advance for the interview were as follows:

- First question: "What are the most prominent cyber threats facing organizations in the Kingdom of Saudi Arabia today, and how have these threats evolved over time?"
- Second question: "How effective are ANNs and RL models in detecting and analyzing cyber-attacks compared to traditional methods?"

- Third question: "What are the main challenges facing the use of AI techniques, such as DL, in enhancing cybersecurity?"
- Fourth question: "How can the accuracy of cyberattack detection systems be improved using DL algorithms, and what factors influence their performance?"
- Fifth question: "In your opinion, what is the future of AI in cybersecurity, and do you see DL as the dominant trend in countering cyber-attacks?"

Validity and reliability of the research tool (interview):

After formulating the interview questions, the tool was reviewed by a panel of specialized experts to evaluate its effectiveness in achieving the research objectives. This assessment focused on ensuring the clarity of each question, the accuracy of its linguistic formulation, and its alignment with the intended purpose. The experts also provided recommendations for improvement, including deletions, additions, rewording, or any other modifications they deemed necessary. After receiving the peer-reviewed copies from the arbitrators and considering their suggestions, the research refined the interview. Some questions were deleted or rephrased based on the consensus of more than 80% of the arbitrators. As a result, after ensuring its face validity, the final version of the interview consisted of seven questions.

Statistical Processing:

The researcher used the "Statistical Package for the Social Sciences - SPSS" application and extracted the data using the following statistical methods: Pearson correlation coefficient, Cronbach's alpha coefficient, frequencies and percentages, arithmetic means and standard deviations, and the range equation, where the response degree was determined to be very low (1), low (2), moderate (3), high (4), very high (5), and the verification degree is determined for each dimension based on the following:

$$\text{Category length} = \frac{Max.limit - Min.limit}{No.of\ levels} = \frac{5-1}{5} = 0.80$$

- A score between 1 and less than 1.80 indicates a very low response.
- A score from 1.80 to less than 2.60 signifies a low response.

- A score from 2.60 to less than 3.40 reflects a moderate response.
- A score from 3.40 to less than 4.20 represents a high response.
- A score from 4.20 to less than 5 denotes a very high response.

Results and Discussion

RQ1: What is the reality of using ANNs in analysing cyber-attacks in the National Cybersecurity Authority in the Kingdom of Saudi Arabia?

To answer this question, the arithmetic means and standard deviations of the statements within the first axis were computed using ANNs for cyber-attack analysis, and these statements were then organized in decreasing order based on the arithmetic mean for each statement, as shown in Table (5).

Table (5): Arithmetic means and standard deviations of the sample individuals' responses to the statements of the first axis: Using ANNs in analysing cyber-attacks

No.	Statement	Arithmetic means	standard deviation	Rank	Responses score
1	Artificial neural networks help to significantly improve the accuracy of detecting cyber-attacks.	3.86	1.259	3	High
2	Artificial neural networks have a high ability to predict cyber-attacks before they occur.	3.48	1.294	9	High
3	Artificial neural networks contribute to improving the speed of response to security incidents.	4.14	1.274	1	High
4	Artificial neural networks have a high classification accuracy for cyber-attacks compared to traditional methods.	3.44	1.351	10	High
5	Artificial neural networks can analyze huge amounts of data quickly and efficiently.	3.82	1.440	4	High
6	Artificial neural networks provide advanced protection against sophisticated cyber-attacks.	3.58	1.592	7	High
7	Artificial neural networks can be easily integrated with traditional intrusion detection systems.	3.95	1.311	2	High
8	Artificial neural networks enable the continuous analysis of threats without the need for frequent human intervention.	3.52	1.636	8	High
9	Artificial neural networks help improve cyber protection strategies through continuous learning.	3.79	1.466	5	High
10	The use of artificial neural networks provides intelligent solutions to confront modern cyber threats.	3.67	1.439	6	High
"Overall average"		3.72	.553	High	

Table (5) indicates that the overall average for the first axis, using ANNs in analyzing cyber-attacks, recorded an arithmetic mean of (3.72) with a standard deviation of (.553), reflecting a (high) response score.

The first axis "Using ANNs in analyzing cyber-attacks" has a response score of "high". This can be explained by the fact that ANNs are better than traditional methods at analyzing large amounts of data, which increases the accuracy of cyberattack detection by identifying suspicious behaviors and abnormal patterns that could be signs of sophisticated cyberattacks. This result is consistent with (Delplace et al., 2020) who confirm that neural networks have remarkable performance when used in the field of cyber security.

ANNs can also adapt to changing cyber threats and continuously learn from new attacks, and help reduce the time required to detect and respond to attacks, which enhances the protection of sensitive systems. In addition, ANNs can be easily integrated with intrusion detection systems and intrusion prevention systems, which enhances the efficiency of these systems.

RQ2: What is the reality of using RL models in analysing cyber-attacks in the National Cybersecurity Authority in the Kingdom of Saudi Arabia?

To answer this question, the arithmetic means and standard deviations of the statements on the second axis were calculated using RL models to analyze cyber-attacks, and these statements were then organized in descending order based on the arithmetic mean of each statement, as shown in Table (6).

Table (6): Arithmetic means and standard deviations of the sample individuals' responses to the statements of the second axis: Using RL models in analyzing cyber-attacks

No.	Statement	Arithmetic means	standard deviation	Rank	Responses score
11	Reinforcement learning models have a high potential to improve cyber-attack detection strategies.	3.53	1.563	8	High
12	Reinforcement learning models improve the accuracy of cyber threat classification over time.	4.11	1.266	3	High
13	Reinforcement learning models help in the early detection of cyber-attacks.	3.74	1.373	6	High

14	Reinforcement learning models are adaptable to changing cyber-attack patterns.	4.18	1.183	2	High
15	Reinforcement learning models can improve cyber defense strategies through continuous learning.	3.65	1.387	7	High
16	Reinforcement learning models provide a dynamic and effective response to various cyber-attacks.	4.05	1.382	4	High
17	Reinforcement learning models support the automation of more intelligent cyber threat detection systems.	3.47	1.494	9	High
18	Reinforcement learning models help improve cyber defense strategies by simulating expected attack scenarios.	4.25	1.167	1	Very High
19	The performance of reinforcement learning models can be improved by using advanced artificial intelligence techniques.	3.42	1.466	10	High
20	Reinforcement learning models help reduce the need for human intervention in threat detection and response.	3.97	1.297	5	High
"Overall average"		3.84	.392	High	

Table (6) indicates that the overall average for the second axis, using RL models in analyzing cyber-attacks, recorded an arithmetic mean of (3.84) with a standard deviation of (.392), additionally a response score of (high). This goes in harmony with Safeer (2025) who confirmed that cybersecurity issues could be addressed with RL. The second axis: Using RL models in analyzing cyber-attacks, obtained a (high) response score, can be explained by the possibility of adapting between RL models and new threats without the need for complete retraining as is the case with some other DL algorithms. These models also have the ability to process huge amounts of data at high speeds, which allows the detection of cyber-attacks in their early stages.

In addition, RL reduces the need for continuous human intervention in analyzing threats and making decisions, as it allows the development of intelligent cyber agents that can act automatically when a potential attack is detected.

Answers from Experts:

Q1: What are the most prominent cyber threats facing organizations in the Kingdom of Saudi Arabia today, and how have these threats evolved over time?

The experts' responses reflect the reality of the advanced cyber threats facing organizations today, as these threats vary between direct technical attacks and attacks that rely on exploiting the human element and AI The analysis of the responses yielded

the following results

The recent attacks show an increasing targeting of energy and communications systems, as attackers are now using advanced technologies such as AI for social engineering. One expert says, "Today we are witnessing a new wave of smart attacks targeting critical infrastructure, which requires the development of defensive solutions based on AI to monitor threats in real time." Ransomware is no longer limited to encrypting data, but rather relies on "double extortion", where data is leaked if the ransom is not paid. A cybersecurity specialist explains this by saying, "Previously, the goal of ransomware was only to encrypt data, but now, attackers threaten to publish sensitive data as an additional means of pressure on victims."

Modern attacks also target DL systems themselves, making them vulnerable to manipulation. As one analyst says, “As AI has evolved, attackers have begun to exploit weaknesses in algorithms, making some cybersecurity systems unable to distinguish real attacks from fake data.”

It is more difficult to identify these attacks early on because large companies are also susceptible to hacking through partners and suppliers. One expert says that attackers have started focusing on suppliers and service providers rather than directly attacking organizations, which makes breach detection more challenging. Attacks on cloud systems are more common as a result of the digital transformation, particularly when security configurations are incorrect. A cloud computing expert claims that many businesses make the mistake of over-trusting their cloud providers while ignoring security settings, which leaves their data open to hacking.

Q2: How effective are ANNs and RL models in detecting and analyzing cyber-attacks compared to traditional methods?

The ability of ANNs to analyze large amounts of data and identify questionable patterns that conventional systems might miss is impressive. Traditional systems are less equipped to handle novel attacks because they are based on pre-established rules, whereas neural networks can continuously learn and identify threats that have not yet

been identified, according to one expert. The capacity to adjust to various situations and enhance performance over time is another feature that distinguishes RL. In a changing environment, RL systems can make proactive decisions based on a dynamic analysis of attacks, which makes them more flexible than traditional systems, according to a cyber researcher.

Compared to conventional intrusion detection systems that depend on predetermined rules, studies reveal that DL techniques achieve accuracy rates in threat detection that surpass 95%. "We found that neural networks excel at detecting hidden attacks that bypass the known signatures of traditional IDS systems when testing them on real data," one analyst noted. Even though these models are effective, they have drawbacks, like the requirement for large amounts of training data and the potential for attack. It is necessary to develop techniques that are resistant to these attacks because, as one expert warns, “Attackers can trick AI models by introducing modified data that makes them make wrong decisions”.

DL methods should be combined with conventional systems for optimal outcomes, according to experts. As stated by one information security expert, “A double layer of protection can be achieved by combining DL algorithms with conventional intrusion detection systems. While traditional systems allow for the detection of known attacks, neural networks and RL allow for the adaptation to new threats”. According to one AI researcher, “These models' ability to analyze attacker behavior and forecast future attacks is a key feature that goes beyond simply identifying threats. By using DL, we can anticipate attacks before they occur, enabling organizations to take preventive action instead of only responding to a breach”

Q3: What are the main challenges facing the use of AI techniques, such as DL, in enhancing cybersecurity?

The analysis's findings demonstrated that while DL models depend on data to identify patterns, hackers can subtly alter that data to fool systems. According to a cybersecurity expert, “attackers can manipulate input data in subtle ways to fool AI

models, which can result in them misclassifying attacks or even evading defenses completely".

DL models' accuracy is primarily determined by the caliber of the data used to train them, but privacy regulations frequently restrict or prevent access to cyberattack data. One AI researcher says, "AI needs huge amounts of accurate data to effectively learn cyber threats, but obtaining up-to-date and reliable data is a major challenge". The decisions made by DL are frequently intricate and difficult for users to understand, even though it is effective at identifying attacks. One information security specialist says, "It can be challenging to elucidate the reasoning behind an AI system's threat identification, which can undermine trust in its findings and complicate the security audit procedure". Additionally, AI algorithms particularly DL need a lot of processing power and sophisticated computer resources.

The difficulty of implementing AI solutions for cybersecurity on a large scale necessitates significant infrastructure investments, which can be prohibitive for small and medium-sized businesses, according to one expert. Although AI is used to bolster cyber defenses, hackers can use it to create increasingly complex attacks. A threat analyst claims "Just as we use AI to detect attacks, attackers have begun using it to develop malware that can adapt to protection systems and to create more convincing phishing attacks".

Q4: How can the accuracy of cyberattack detection systems be improved using DL algorithms, and what factors influence their performance?

The analysis results revealed that the effectiveness of DL algorithms is primarily driven by the quality and diversity of the training data. One expert in AI indicated that "to enhance detection accuracy, models must be trained on data containing different types of cyber-attacks, including recent, unknown attacks." The accuracy of models can also be improved by using advanced neural network architectures such as neural networks or long-term memory networks, which are characterized by their ability to capture temporal patterns in cyber-attacks. One researcher said, "Advances in neural

network design allow for a deeper analysis of attack behavior, which enhances the ability of systems to distinguish between normal activity and malicious attacks."

Continuously updating AI models using adaptive learning and RL helps improve their performance over time. One expert points out that "AI should not be static; it should be updated periodically with new data to ensure its ability to deal with modern attacks." Hybrid systems that combine AI and traditional methods are also more accurate. One cybersecurity specialist says, "Relying exclusively on AI may not be enough, but when combined with traditional intrusion detection systems, we get a higher and more balanced level of protection."

The "black box" problem in AI is considered a major challenge, upon this using explainable AI (XAI) techniques helps improve the accuracy of models and increases users' confidence in them. One analyst says, "When we understand why AI makes certain decisions, we can improve and correct it when needed, which enhances its accuracy."

Q5: In your opinion, what is the future of AI in cybersecurity, and do you see DL as the dominant trend in countering cyber-attacks?

The results of the analysis of responses concerning the future of AI in cybersecurity indicated that there is increasing reliance on AI in cyber defense. As cyber threats become more complex, AI has become an essential tool in detecting, analyzing, and responding to threats in real time. Due to its superior analytical capabilities over conventional techniques, one expert notes that "big organizations have started to rely on AI as a key element in cyber defense strategies". AI will develop to become more proactive, predicting attacks before they happen, as opposed to merely tracking them after they happen. According to a cybersecurity expert, "AI will evolve from a defensive tool to a proactive system that can predict cyberattacks before they happen, significantly lessening their impact".

According to one researcher, "while it will not take the place of people, AI will be a useful tool for efficient data analysis and security decision-making. The integration of

AI and human experts, where AI analyzes large data while humans make strategic decisions, is where the future lies". Responses showed that DL can analyze large amounts of data and identify unknown attacks, but it has drawbacks like requiring a lot of computing power and data. Despite this, DL may be the standard method for thwarting cyberattacks. While DL is effective at detecting attacks, one expert pointed out that its high cost and requirement for up-to-date training data could prevent its widespread use. To improve results, DL will be used in conjunction with methods like behavioral analysis, rule-based systems, and RL rather than solely depending on it. One researcher stated that "hybrid systems that integrate AI, human analysis, and conventional security techniques are the way of the future rather than relying solely on DL". Because it can better adjust to novel and evolving attacks, RL might occasionally be a better option than DL. According to one researcher, "RL, which depends on systems' experience and the ability to learn from mistakes in dynamic environments, may perform better than DL in some cybersecurity scenarios".

Conclusion

- The study concluded that the reality of using ANNs in analysing cyber-attacks in the National Cybersecurity Authority in the Kingdom of Saudi Arabia obtained a (high) response score.
- The reality of using RL models in analyzing cyber-attacks in the National Cybersecurity Authority in the Kingdom of Saudi Arabia recorded a (high) response score.

Limitations

- Limiting model effectiveness due to insufficient, homogeneous training datasets for diverse cyber-attack detection.
- Lacking transparency in DL decisions, reducing trust and interpretability in cybersecurity applications.
- Increased vulnerability to adversarial attacks and high computational requirements hinders real-time deployment.

Recommendations

- Providing large and diverse datasets that include different cyber-attack patterns to develop the accuracy of models.
- Using data processing techniques such as data cleaning and even distribution to reduce the problem of imbalanced data.
- Integrating RL algorithms with generative AI models to create advanced defense strategies against unknown cyber-attacks.
- Monitoring and analyzing model vulnerabilities to prevent their exploitation by cyber attackers.
- Periodically updating models to ensure their effectiveness in confronting modern cyber threats.
- Integrating DL algorithms with intrusion detection and prevention systems to enhance the performance of cyber defenses.
- Providing flexible programming interfaces to connect DL algorithms with existing cybersecurity platforms.
- Designing offensive and defensive test labs to test the effectiveness of ANNs and RL models.
- Using simulated data of cyber-attacks to increase the efficiency of models before deploying them in real environments.
- Developing RL-based simulation tools to automatically anticipate and respond to attack scenarios.
- Training cybersecurity professionals to use and develop advanced AI algorithms.
- Incorporating academic curricula and professional programs that focus on DL applications in cyber-attack analysis.

References

- Abouhawwash, M. (2024). Innovations in Cyber Defense with Deep Reinforcement Learning: A Concise and Contemporary Review. Artificial Intelligence in Cybersecurity, 1, 44–51.
- Al-Dhamen, M. (2007). Basics of Scientific Research. 1st ed., Amman: Dar Al-Masirah for Publishing and Distribution.

- Al-Nawashi, M. M., Al-hazaimeh, O. M., Tahat, N. M., Gharaibeh, N., Abu-Ain, W. A., & Abu-Ain, T. (2025). Deep Reinforcement Learning-Based Framework for Enhancing Cybersecurity. International Journal of Interactive Mobile Technologies, 19(3).
- Alzhrani, A. A., Alghamdi, R., Salawi, A., Alghamdi, W. A., & Alghamdi, M. I. Comparison between Saudi Arabia and USA: Prevention and Dealing with Cyber Security.
- Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the effectiveness of machine and deep learning for cyber security. 2018 10th international conference on cyber Conflict (CyCon),
- Azam, Z., Islam, M. M., & Huda, M. N. (2023). Comparative analysis of intrusion detection systems and machine learning-based model analysis through decision tree. IEEE Access, 11, 80348–80391.
- Bapiyev, M., Aitchanov, B. H., Tereikovskyi, A., Tereikovska, L. A., & Korchenko, A. A. (2017). Deep neural networks in cyber attack detection systems.
- Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. Information, 10(4), 122.
- CYBERSECURITY, A. A COMPREHENSIVE SURVEY ON EXPLAINABLE AI IN CYBERSECURITY DOMAIN.
- Dahl, G. E., Sainath, T. N., & Hinton, G. E. (2013). Improving deep neural networks for LVCSR using rectified linear units and dropout. 2013 IEEE international conference on acoustics, speech and signal processing,
- Delplace, A., Hermoso, S., & Anandita, K. (2020). Cyber attack detection thanks to machine learning algorithms. arXiv preprint arXiv:2001.06309.
- Fintech Saudi Deep Dives: Cybersecurity Solution Opportunities in KSA. Deloitte & Touche. (2021).
- Ghazal, S. F., & Mjlae, S. A. (2022). Cybersecurity in deep learning techniques: detecting network attacks. International Journal of Advanced Computer Science and Applications, 13(11).
- Gjylapi, D., Proko, E., & Gjylapi, S. ARTIFICIAL NEURAL NETWORKS IN CYBER SECURITY.
- Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. Advances in neural information processing systems, 27.
- Halbouni, A., Gunawan, T. S., Habaebi, M. H., Halbouni, M., Kartiwi, M., & Ahmad, R. (2022). Machine learning and deep learning approaches for cybersecurity: A review. IEEE Access, 10, 19572–19585.

- Hernandez-Suarez, A., Sanchez-Perez, G., Toscano-Medina, L. K., Perez-Meana, H., Olivares-Mercado, J., Portillo-Portillo, J., Benitez-Garcia, G., Sandoval Orozco, A. L., & García Villalba, L. J. (2023). ReinforSec: an automatic generator of synthetic malware samples and denial-of-service attacks through reinforcement learning. Sensors, 23(3), 1231.
- Hihi, S., & Bengio, Y. (1995). Hierarchical recurrent neural networks for long-term dependencies. Advances in neural information processing systems, 8.
- KABANDA, G., CHIPFUMBU, C. T., & CHINGORIWO, T. (2023). A Reinforcement Learning Paradigm for Cybersecurity Education and Training. Oriental Journal of Computer Science and Technology, 12–45.
- Li, G., Sharma, P., Pan, L., Rajasegarar, S., Karmakar, C., & Patterson, N. (2021). Deep learning algorithms for cyber security applications: A survey. Journal of Computer Security, 29(5), 447–471.
- Mousavi, S., Schukat, M., & Howley, E. (2018). Researching advanced deep learning methodologies in combination with reinforcement learning techniques Master's thesis, National University of Ireland Galway].
- Muheidat, F., Mallouh, M. A., Al-Saleh, O., Al-Khasawneh, O., & Tawalbeh, L. a. A. (2024). Applying AI and Machine Learning to Enhance Automated Cybersecurity and Network Threat Identification. Procedia Computer Science, 251, 287–294.
- Nguyen, T. T., & Reddi, V. J. (2021). Deep reinforcement learning for cyber security. IEEE Transactions on Neural Networks and Learning Systems, 34(8), 3779–3795.
- Oh, S. H., Jeong, M. K., Kim, H. C., & Park, J. (2023). Applying reinforcement learning for enhanced cybersecurity against adversarial simulation. Sensors, 23(6), 3000.
- Okafor, M. O. (2024). Deep learning in cybersecurity: Enhancing threat detection and response.
- Podder, P., Bharati, S., Mondal, M., Paul, P. K., & Kose, U. (2021). Artificial neural network for cybersecurity: A comprehensive review. arXiv preprint arXiv:2107.01185.
- Qamar, R., & Zardari, B. A. (2023). Artificial neural networks: An overview. Mesopotamian Journal of Computer Science, 2023, 124–133.
- Safeer, E. (2025). Reinforcement Learning Approaches in Cyber Security. In Reshaping CyberSecurity With Generative AI Techniques (pp. 53–76). IGI Global.
- Samia, N. K. (2023). Global Cyber Attack Forecast using AI Techniques The University of Western Ontario (Canada)].
- Sarker, I. H. (2021). Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions. SN computer science, 2(6), 1–20.
- Thomas, T., Vijayaraghavan, A. P., & Emmanuel, S. (2019). Machine learning approaches in cyber security analytics. Springer.

- Tian, Y., Shu, M., & Jia, Q. (2022). Artificial neural network. In Encyclopedia of Mathematical Geosciences (pp. 1–4). Springer.
- Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. IEEE Access, 6, 35365–35381.