Babylonian Journal of Networking
Vol.2023, **pp.** 21-28
DOI: https://doi.org/10.58496/BJN/2023/004; ISSN: 3006-5372
https://mesopotamian.press/journals/index.php/BJN/index

Research Article

A Survey on the Significance of Artificial intelligence (AI) in Network cybersecurity

Maryam Abdulsalam Ali[1,*], Ali Alqaraghuli [2]

[1]*Information Science and Technology, UKM, Malaysia.*
[2]*Electrical and Computer Engineering, Altinbas University, İstanbul, Türkiye*

A R T I C L E I N F O

Article History
Received 04 Feb 2023
Accepted 02 Apr 2023
Published 21 Apr 2023

Keywords
Artificial intelligence
Machine Learnig
Deep Learning
Cyber-security
Data Science
Algorithms

ABSTRACT

Virtual environments providing public services, private businesses, and social media platforms occupy a large portion of our time. Cybercriminals should refrain from stealing data or compromising systems in these settings. Cybersecurity refers to the actions taken at the executive, organisational, and technological levels to protect data, communication networks, and electronic information from unauthorised access, use, or disclosure. Additionally, it must manage all necessary criteria to safeguard customers from dangers and intrusions while simultaneously improving the security, privacy, and secrecy of personal data. The literature reviewed here focuses on artificial intelligence (AI) as it relates to cybersecurity, protecting computer systems from assault, hacking, and data theft. An overview of seminal works on the topic of deep learning and machine learning as they pertain to cybersecurity is provided in this study. Machine learning and deep learning algorithms also regulate computer system infiltration by predicting and understanding harmful software behavior and traffic, which protects against illegal admission.

1. INTRODUCTION

The advent of the internet has facilitated the global exchange of knowledge and cultures, effectively transforming the world into a closely interconnected community. The functionality of the internet, computers, and mobile phones is contingent upon the presence of networks. Networks facilitate the flow of data, information, and applications among computers using various means such as cables and radio waves. The protection of personal information is of paramount importance when transmitted across networks, as it is susceptible to exploitation by malicious individuals seeking to engage in identity theft or the creation of deceptive social networking profiles [1]. Following the COVID-19 pandemic, there has been a widespread adoption of digital transactions that aim to minimise physical contact [2],[3]. The COVID-19 epidemic has prompted numerous organisations and enterprises to adopt paperless practises. Research has demonstrated that electronic transactions offer superior functionality and increased accessibility. The prevalence of online shopping has witnessed a significant surge facilitated by platforms such as Facebook and various applications that facilitate the promotion and purchase of goods. Similarly, e-education and training initiatives have gained momentum in universities, institutes, and even schools. These activities have experienced rapid growth and have become increasingly sought-after, particularly in light of the widespread adoption of remote work in both public and private sectors [4], [5]. The coexistence of individuals within the same organisation in a shared work environment, facilitated by remote work arrangements, working in public spaces such as cafeterias or restaurants, and utilising a single computer for both business and personal transactions, necessitates a thorough evaluation of the associated business risks by those responsible for information security. The implementation of remote work practises has been shown to effectively reduce instances of attacks and hacks perpetrated

* *Corresponding author. Email: XXXX@XXXX.com*

by individuals who are not physically present in the same work environment [6], [7]. Despite the implementation of sophisticated technical security measures by the organisation to mitigate cyber threats, it is imperative to prioritise the human factor, which represents the most vulnerable component within this framework. Consequently, there is a need to enhance the capabilities of employees in order to address this vulnerability. Unauthorised access and malicious software have the potential to surreptitiously extract or erase data without the user's awareness. In order to mitigate risks, it is imperative to implement a comprehensive approach that encompasses both awareness initiatives, such as training and workshops targeting employees with low levels of awareness, as well as technology solutions. The failure of employees to adhere to information security protocols, such as neglecting to lock their computers when leaving their workstations, keeping computer screens on while engaging in conversations or using mobile devices in public areas, and disregarding business standards by entering passwords on their devices, poses a significant risk to information security. The widespread accessibility of information without significant barriers poses a risk by potentially enabling unauthorised access, hence aiding cyber-attacks and compromising data security. The assessment of hazards associated with remote work is necessary due to the following factors. The methods used by artificial intelligence are cutting edge and very useful. Cyber and information security rely on these tactics [8, 9]. Electronic gadgets, software, apps, and gaming consoles can mimic human cognition, memory, and data processing with the help of artificial intelligence [10]. These methods make use of experimental results. Machines with electronic brains that can process data and carry out tasks are what we call AI-enabled devices. The term "cybersecurity" has only recently emerged, thanks to the proliferation of high-speed Internet (1G, 4G, etc.) and the ease with which people may access it [11]. In order to commit electronic crimes, unauthorised individuals can take applications, data, and information from computers and other electronic devices. Businesses rely on AI to foretell cyberattacks, crimes, and computer breaches. If they are more trustworthy than experts, authorised users can access network data using AI methods. These methods will be a time saver for specialists since they are good learners, remembers, and finishers. AI methods perpetuate patterns even after they are no longer conceived of [12], [13]. The cybersecurity function records the habits and actions of every user. Predicting malware penetration using these methods is possible by analysing user behaviour and practises [14], [15].

2. PRACTICES OF THE CYBERSECURITY

Over the past few years, there has been a significant expansion and integration of the electronic gadgets and technology sector, which has become indispensable in our daily existence. The completion of business and projects is contingent upon its presence. Contemporary technological equipment necessitate applications that cater to the needs of humans while also ensuring safeguards against invasions, hacking, attacks, and unauthorised entrance. Numerous organisations and institutions express concerns regarding the potential risks of hacking and data theft, since they are compelled to safeguard their systems and data [16]. The reference provided is in the form of a numerical citation, indicating that the user is referring Data plays a crucial role in the operations of companies and institutions. The topic of cybersecurity is a significant concern across several industries in contemporary times. Cybersecurity encompasses a range of measures aimed at safeguarding the communication systems, data, and raw information of organisations or institutions. This includes ensuring the security of both virtual and physical components of operating systems, as well as securing applications that are essential for the system's functioning and restricted to authorised individuals [18-20]. Cybersecurity is a range of methodologies and techniques employed to safeguard computer networks and data against unauthorised access, malicious attacks, and theft. The process include the examination of electronic hazards, the protection of computer data, and the management of malicious software [21]. The field of cybersecurity is responsible for safeguarding the confidentiality of computer systems, thereby thwarting any attempts to gain unauthorised access to or manipulate data. Integrity serves as a safeguard against intentional alterations or deletions of data with harmful intent. The concept of availability pertains to the assurance that data, information, and communications are accessible to authorised individuals, thereby preventing unauthorised parties from illicitly obtaining or comprehending them. Irrespective of the location of a cyber-attack, it is certain that it will inflict harm upon the organisation, its staff, and its customers. Educating staff on the subject of cybersecurity is crucial in order to mitigate errors and safeguard against unauthorised access to computer systems. Table 1 provides an overview of the principal cyberthreats.

TABLE I. Categories of Cybersecurity Attacks

Narrative	**Cybersecurity Attack Type**
Numerous malicious applications attempt to inflict harm on systems and pilfer data.	Malware
Characterized as malicious software, it strives to encrypt data, disable systems, and deny authorized users access.	Ransomware
An established form of social engineering aimed at manipulating individuals to undertake unsafe actions and disclose their data and sensitive information online.	Phishing
Primarily designed to incapacitate systems and hinder user access to network resources, leading to financial or reputational harm to the institution or company.	DDoS (Distributed Denial of Service)
Exploiting a security vulnerability on the web, an unauthorized individual gains access to the site's data, enabling theft, modification, or deletion of information, resulting in website dysfunction.	SQL Injection
The art of manipulating and deceiving people, wherein the attacker leverages known passwords to facilitate unauthorized access, data theft, and the installation of malicious software.	Social Engineering

In the seventies, the first malicious software appeared in history named Creeper, a program that destroys computer data in order to delete all data, and it showed a note on the screen "I'm a creeper, catch me if you can!", (see Figure 1). And then, the first antivirus appeared called Reaper, and its primary function was to destroy Creeper.

Fig. 1. Message from Creeper was the first malware in history.

The inaugural hacker in history was Nevil Maskelyne (refer to Figure 2.a). In 1903, he intercepted the inaugural wireless telegraph message, therefore exposing the susceptibilities inherent in Marconi's devised technology. John Draper, often known as Captain Crunch, is recognised as the pioneer of cybercrime (see to Figure 2.b). Draper found that the whistle included in "Cap'n Crunch" cereal boxes might deceive the telephone exchange signal, enabling the creation of free calls.

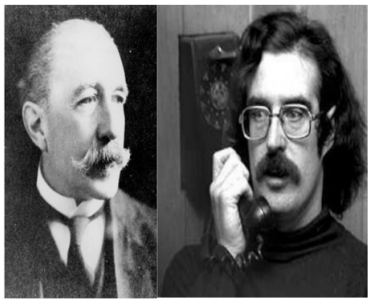

Fig. 2. Oldest hacker in the world :(a) Nevil Maskelyne (b) John Draper.

3. CYBERSECURITY DATA SCIENCE

Data can be transformed into numbers in many different fields, including cybersecurity, retail, and the life sciences. Cybersecurity and system development both depend significantly on data, making data science an essential component. By examining security data collected from users and network personnel, cyber dangers can be identified. To determine where data is coming from when it enters a network, cybersecurity professionals employ tools including file hashes, signatures, custom-written rules, and heuristics. Manual methods have their advantages, but they're not equal to the task of defending against cyber threats. As seen in Figure 3, decision-making is impacted by massive data. Plus, cyberpatients. With data science, we hope to enhance information technology. Finding and fixing security holes in a system is possible with the use of machine learning and deep learning. Data science and artificial intelligence have been crucial in cybersecurity over the past decade, helping to turn raw data into decisions and secure systems that were previously vulnerable. Data science streamlines processes and decision-making. Data science employs various methods to transform massive amounts of data into actionable insights, such as:

a. Data engineering focuses on the development and implementation of systems that collect and analyse data.
b. Aid in the reduction of data volume by selectively filtering essential and relevant data.
c. Utilise methodologies to identify distinctive patterns and get knowledge from data.
d. Developing cutting-edge security models based on data analysis.
e. New security alerts enhance understanding of the manipulated tactics used to minimise false alerts.
f. Enhancing and expanding the resources within the system.

Fig. 3. A straightforward explanation of how decisions are made based on data analysis.

4. MACHINE LEARNING IN CYBERSECURITY

Electronic devices are increasingly becoming popular and are being utilised in diverse domains. Data theft and cyber threats might result from an excessive exchange of information across technological devices. The advancement and utilisation of technology have a direct impact on the magnitude of dangers encountered. Machine learning methods are always advancing and expanding, prompting numerous studies to recommend their utilisation in addressing electronic threats. Cyber threats exhibit diversity and undergo changes throughout time, giving rise to novel forms of data theft. Machine learning is the most effective method for mitigating cyberattacks [22], [23]. Machine learning algorithms possess the ability to adjust and acquire knowledge. While AI and ML surpass existing cybersecurity solutions in their ability to identify, control, and prevent known malware attacks, many styles of cyberattacks remain unanswered by these technologies. Machine learning is the predominant field within the realm of artificial intelligence. Data analytics is a collection of statistical procedures that aims to analyse data, identify new characteristics, and assist in decision-making. Machine learning enables computers to learn from data inputted by experts [24]. Machine learning techniques are employed to discover novel data patterns or predict forthcoming activities. Cybersecurity use these tactics. Supervised and unsupervised methods are prevalent. Although machine learning has seen significant advancements in the field of cybersecurity, these technologies are not flawless as they still necessitate human oversight. Moreover, algorithms must be periodically retrained due to the inability to entirely automate data processing [25], [26]. This section provides an analysis of the intersection between machine learning and cybersecurity. Figure 4 illustrates the process by which machine learning identifies abnormalities in a system.

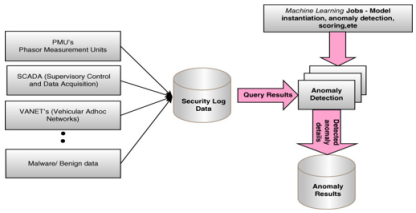

Fig. 4. Detecting anomaly through machine learning techniques.

4.1 Supervised Learning in Cybersecurity

To accomplish certain objectives, supervised learning makes use of inputs [27]. Since they are simple to implement and keep tabs on, supervised learning techniques have found widespread use in fields as diverse as medicine and security. To categorise security data or foresee a possible security issue, these methods are employed. For instance, if a company's computer or service is targeted by an attack and unwanted messages keep popping up on the screen, making it impossible to delete them, the company might be unable to continue forward with its job, perhaps losing money or data and being unable to get it back (see Figure 5). Any industry can benefit from machine learning methodologies when it comes to data and user security. Logistic regression, decision trees, support vector machines, k-nearest neighbours, and nave bayes are the most important supervised learning techniques for classification. These techniques are also used for prediction because they can build a data-based predictive model. For example, collecting data on an ong or predicting the activities of users in a specific network within a public or private institution. By applying supervised learning techniques like linear regression and support vector regression, we might potentially identify fraud and develop ways to eradicate it, as well as uncover the causes of serious cybercrimes that impact a large number of people and are among the most harmful crimes currently in existence. A lot of people are confused between regression and classification. Regression results are numerical and continuous, whereas classification results are more discrete and categorical.

Fig. 5. Using machine learning techniques, identify potentially harmful or benign datasets.

4.2 Unsupervised Learning in Cybersecurity

Finding information, structures, or patterns in unlabeled data is the goal of unsupervised learning methods. Malware constantly adapts its behaviour in order to evade detection and potential fixes in cybersecurity [28]. To discover and understand complex and hidden assaults, clustering methods (such as K-means, K-medoids, and single linkage) employ unsupervised learning. In order to alert users or programmers of system abnormalities, privacy policy violations, or unauthorised data, unsupervised learning approaches search. Furthermore, regardless of the size of the dataset, functional tasks such as optimising the dataset's characteristics or identifying the key aspects for a certain security concern are inherent in these technologies and present themselves in the course of additional research. We also prioritise security. Along with other methods, such as principal component analysis, linear discriminant analysis, non-negative matrix factorization, and Pearson correlation analysis, cyber dangers can be solved and hidden programmes can be detected as machine learning rules to prevent attacks and data theft. The rules of an expert system are determined by hand by a data security expert and a knowledge engineer. One way to extract security-related characteristics or properties is through association rules learning, which finds rules or relationships between datasets. Analysing the correlations between datasets is what correlation analysis is all about. There are various data mining methodologies, such as those based on patterns, logic, trees, and more. Apriori, Apriori-TID, Eclat, FP-Tree, RARM, AIS, and Apriori-Hybrid Methods in cybersecurity establish guidelines for linking regulations pertaining to data theft and penetration. There are threats that machine learning cannot identify. Since it wasn't present until the system was attacked, these techniques are unable to detect it. If the policy is overly general, it could result in vulnerabilities or false positives when trying to detect patterns of behaviour. Malware or unauthorised

data can be detected by these methods. If a cybersecurity machine learning technique is to be trained on the full dataset that will be monitored, dataset selection is crucial. This technique will then be able to forecast attacks or alert of malware entering the system. You need to acquire these skills before you begin working. Lacking proper training, the outcomes are inaccurate. There is documentation of threats and attacks. Avoid using machine learning to detect uncommon dangers. In order to hack, steal data, and circumvent security systems using just one defensive technique, cybercriminals take use of system flaws. There should be a wide variety of supplementary methods in a cybersecurity system that relies on machine learning.

4.3 Deep Learning in Cybersecurity

A number of factors, including data volume, problem type, issue sensitivity, and tolerance for solution decisions, determine whether cybersecurity tactics are considered acceptable. Massive datasets are no match for deep learning methods built on parallel processing [29–32]. The security, privacy, and reliability of data, as well as its absence of unauthorised access, are guaranteed by using deep learning architectures on server-based systems. Deep learning for cybersecurity has two stages. Get the local data transit encrypted before sending it to the server. The second step is to identify the data type and then submit the information to the server for classification. In data classification, this step is critical for character recognition in images; the previous step involves character encoding and transmission; the current step involves data processing and the identification of a man-in-the-middle attack between the server and local system. So, no unauthorised individuals can access the data while it is being transmitted to the users. A system for fingerprint and face identification can be seen in Figure 6.

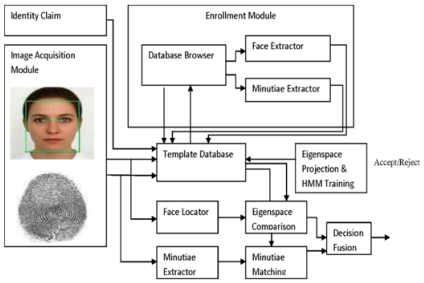

Fig. 6. Scheme of how to develop a system for face recognition and fingerprint.

5. CONCLUSIONS AND FUTURE DIRECTIONS

With the potential to enhance services and technologies for everybody, artificial intelligence (AI) is a prominent scientific field that is expected to experience tremendous growth and development. Explore artificial intelligence and cybersecurity to find a middle ground between the proliferation of electronic gadgets and human values. Virtual worlds and social media platforms must employ cutting-edge technologies to protect user privacy. Hence, when discussing the future and advancements in AI capabilities, it is important to keep up with the rapid growth of this field in cybersecurity, develop AI-dependent applications, activate international digital cooperation, and reap the benefits of digital technology transfer and physical environment integration. Researchers should have unfettered access to additional data for the purpose of training and analysing AI systems, without restrictions or compromises to user privacy. Maintaining funding for deep learning and machine learning studies is crucial to protecting the personal information of social media users. A large number of cybersecurity experts keep up with the newest developments in the field, including new software, hardware, and methods used by hackers and viruses. There will be fines and punishments for using AI for malicious purposes and revealing users' personal information in due time. In upcoming articles, we will discuss how to utilise machine learning and deep learning to categorise and predict cybersecurity data.

Conflicts Of Interest

None

Funding

None

Acknowledgment

None

References

[1] B. N. Bhalaji, "Reliable Data Transmission with Heightened Confidentiality and Integrity in IOT Empowered Mobile Networks," Journal of IoT in Social, Mobile, Analytics, and Cloud, vol. 2, no. 2, pp. 106–117, May 2020.
[2] J. Budd et al., "Digital technologies in the public-health response to COVID-19," Nature Medicine, vol. 26, pp. 1183–1192, Aug. 2020.
[3] K. Leung, J. T. Wu, and G. M. Leung, "Real-time tracking and prediction of COVID-19 infection using digital proxies of population mobility and mixing," Nature Communications, vol. 12, no. 1501, pp. 1–8, Mar. 2021.
[4] S. Shrestha, S. Haque, S. Dawadi, and R. A. Giri, "Preparations for and practices of online education during the Covid-19 pandemic: A study of Bangladesh and Nepal," Education and Information Technologies, vol. 27, pp. 243–265, Jul. 2021.
[5] M. Ssenyonga, "Imperatives for post COVID-19 recovery of Indonesia's education, labor, and SME sectors," Cogent Economics Finance, vol. 9, no. 1, pp. 1–51, Apr. 2021.
[6] H. Saleous et al., "COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities," Digital Communications and Networks, in press, Jun. 2022.
[7] H. S. Lallie et al., "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," Computers Security, vol. 105, pp. 102248, Jun. 2021.
[8] J. Li, "Cyber security meets artificial intelligence: a survey," Frontiers of Information Technology Electronic Engineering, vol. 19, pp. 1462–1474, Jan. 2019.
[9] Z. Zhang et al., "Artificial intelligence in cyber security: research advances, challenges, and opportunities," Artificial Intelligence Review, vol. 55, pp. 1029–1053, Mar. 2021.
[10] M. M. Mijwil, "Implementation of Machine Learning Techniques for the Classification of Lung X-Ray Images Used to Detect COVID-19 in Humans," Iraqi Journal of Science, vol. 62, no. 6, pp. 2099-2109, Jul. 2021.
[11] J. Cáceres-Hidalgo and D. Avila-Pesantez, "Cybersecurity Study in 5G Network Slicing Technology: A Systematic Mapping Review," in Proc. IEEE Fifth Ecuador Technical Chapters Meeting, pp. 1–6, Oct. 2021.
[12] T. Ghosh et al., "Artificial intelligence and internet of things in screening and management of autism spectrum disorder," Sustainable Cities and Society, vol. 74, pp. 103189, Nov. 2021.
[13] A. Adadi, M. Lahmer, and S. Nasiri, "Artificial Intelligence and COVID-19: A Systematic umbrella review and roads ahead," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 8, pp. 5898-5920, Sep. 2022.
[14] M. Abdullahi et al., "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review," Electronics, vol. 11, no. 2, pp. 1-27, Jan. 2022.
[15] I. F. Kilincer, F. Ertam, and A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," Computer Networks, vol. 188, pp. 107840, Apr. 2021.
[16] S. Kuipers and M. Schonheit, "Data Breaches and Effective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises," Corporate Reputation Review, vol. 25, pp. 176–197, Aug. 2021.
[17] N. Rawindaran et al., "Cost Benefits of Using Machine Learning Features in NIDS for Cyber Security in UK Small Medium Enterprises (SME)," Future Internet, vol. 13, no. 8, pp. 1-36, Jul. 2021.
[18] F. Quayyum, D. S. Cruzes, and L. Jaccheri, "Cybersecurity awareness for children: A systematic literature review," International Journal of Child-Computer Interaction, vol. 30, pp. 100343, Dec. 2021.
[19] P. Formosa, M. Wilson, and D. Richards, "A principlist framework for cybersecurity ethics," Computers Security, vol. 109, pp. 102382, Oct. 2021.
[20] I. H. Sarker, H. Furhad, and R. Nowrozy, "AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions," SN Computer Science, vol. 2, no. 173, Mar. 2021.
[21] E. Fosch-Villaronga and T. Mahler, "Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots," Computer Law Security Review, vol. 41, pp. 105528, Jul. 2021.
[22] T. S. R. and Sathya R., "Ensemble Machine Learning Techniques for Attack Prediction in NIDS Environment," Iraqi Journal For Computer Science and Mathematics, vol. 3, no. 2, pp. 78–82, Mar. 2022.
[23] Y. Niu and A. Korneev, "Identification Method of Power Internet Attack Information Based on Machine Learning," Iraqi Journal For Computer Science and Mathematics, vol. 3, no. 2, pp. 1–7, Feb. 2022.
[24] M. M. Mijwil and E. A. Al-Zubaidi, "Medical Image Classification for Coronavirus Disease (COVID-19) Using Convolutional Neural Networks," Iraqi Journal of Science, vol. 62, no. 8, pp. 2740-2747, Aug. 2021.

[25] M. Sarhan et al., "Feature extraction for machine learning-based intrusion detection in IoT networks," Digital Communications and Networks, in press, Sep. 2022.
[26] M. A. Teixeira et al., "SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach," Future Internet, vol. 10, no. 8, pp. 1-15, Aug. 2018.
[27] K. Aggarwal et al., "Has the Future Started? The Current Growth of Artificial Intelligence, Machine Learning, and Deep Learning," Iraqi Journal for Computer Science and Mathematics, vol. 3, no. 1, pp. 115-123, Jan. 2022.
[28] L. F. Maimó et al., "Intelligent and Dynamic Ransomware Spread Detection and Mitigation in Integrated Clinical Environments," Sensors, vol. 19, no. 5, pp. 1-31, Mar. 2019.
[29] S. Ahmed et al., "Speaker Identification Model Based on Deep Neural Networks," Iraqi Journal For Computer Science and Mathematics, vol. 3, no. 1, pp. 108-114, Jan. 2022.
[30] R. Qamar et al., "Survey on Generative Adversarial Behavior in Artificial Neural Tasks," Iraqi Journal For Computer Science and Mathematics, vol. 3, no. 2, pp. 83-94, Mar. 2022.
[31] A. K. Faieq and M. M. Mijwil, "Prediction of Heart Diseases Utilising Support Vector Machine and Artificial Neural Network," Indonesian Journal of Electrical Engineering and Computer Science, vol. 26, no. 1, pp. 374-380, Apr. 2022.
[32] M. M. Mijwil, R. A. Abttan, and A. Alkhazraji, "Artificial intelligence for COVID-19: A Short Article," Asian Journal of Pharmacy, Nursing and Medical Sciences, vol. 10, no. 1, pp. 1-6, May 2022.