INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 14, Issue 4, (2024) E-ISSN: 2222-6990

# The Role of Artificial Intelligence in Addressing Cybersecurity Challenges

Maitha Musabah Salem Bin Dawi Alkhatri and Diaya Uddeen Deab Mahmoud Alzitawi

Islamic Civilisation Academy, Faculty Social Science and Humanities, Universiti Teknologi Malaysia (UTM)

Email: musabahsalem@graduate.utm.my, diaya@utm.my

**To Link this Article:** http://dx.doi.org/10.6007/IJARBSS/v14-i4/21312 DOI:10.6007/IJARBSS/v14-i4/21312

***Published Date:*** 06 April 2024

**Abstract**

Today's digital age presents more complex cyber dangers, and enterprises have the onerous burden of safeguarding critical information and infrastructure from unwanted actors. With the growth of the cyber landscape, the defense strategy must also adapt. This study tries to identify the role of artificial intelligence in tackling cyber issues, and it uses the descriptive deductive technique. Thus, the study arrived at a number of important conclusions, the most significant of which are as follows: artificial intelligence can enhance cybersecurity by refining attack detection protocols, analyzing network behaviors, and creating intelligent security systems that can effectively counteract emerging threats. Artificial intelligence can also analyze big data related to network activities and digital behaviors to anticipate and identify potential vulnerabilities and future attacks.

**Keywords:** Artificial Intelligence, Cyber Security, Cyber Challenges, Cybercrime, Combating Cybercrime

## Introduction

Today's digital age presents enterprises with the difficult challenge of defending their infrastructure and sensitive data from malevolent individuals as cyber threats get more sophisticated. The defensive plan needs to change along with the cyber environment.

Artificial intelligence (AI) is a potential technology that has surfaced as a substitute for the cybersecurity game rules. Artificial Intelligence (AI) provides creative ways to bolster our defenses by analyzing massive volumes of data and learning from trends. This essay delves into the intriguing realm of artificial intelligence, examining its inventive applications and cybersecurity obstacles.

Information and communication systems exposed to the Internet are shielded from risks and harmful attacks by cybersecurity (Li & Liu, 2021). Cybersecurity is now multifaceted, spanning from network and application security to infrastructure, cloud, and information

security thanks to the Fourth Industrial Revolution and the Industrial Internet of Things (IIoT) (Yu & Guo, 2019).

Rather than being restricted to system security alone, cybersecurity encompasses a wide range of interrelated technologies and components in cyberspace. Cybersecurity also entails simultaneously safeguarding all pertinent aspects of cyberspace (Li & Liu, 2021).

The study is important because it addresses the growing cyber threats that modern governments and organizations face, which call for strong defense and confrontation tactics. Cyber threats continue to pose a serious threat to cyber security despite the world's technological advancements. These threats include data theft, malware, cyber breaches, electronic fraud, and hybrid threats that make use of contemporary technologies like artificial intelligence and machine learning. It can use neuroscientific methods or techniques to study consumer behavior (Ahmed et al., 2022; Alsharif et al., 2022; 2023a; 2023b). These techniques such as neuroimaging and physiological techniques (Alsharif et al., 2021a; 2021b; 2021c). Furthermore, these techniques can map the consumer unconscious behavior (Halsharif et al., 2020; 2021a; 2021b; 2023; Pilelienė et al., 2022).

Since the analysis and processing of the vast amounts of data generated by malicious cyber activities require specialized knowledge and skills, the primary issue is the inability to respond to these threats effectively and promptly. Therefore, the key question is: What role does artificial intelligence play in responding to cyber challenges? Furthermore, because cyber threats are constantly evolving due to the advancement of the technologies employed in them, it is challenging for traditional systems to keep up with these difficulties and offer sufficient protection. Artificial intelligence can analyze and resolve cyber challenges by applying a descriptive and deductive approach.

## Literature Review

### *Artificial Intelligence*

All living things have neurological systems, which allow them to interact and cope with their surroundings as well as help them govern the essential functions required for these creatures to continue to live. Different creatures have different neural systems; higher organisms like humans have complex neural systems that are natural, while protozoa organisms with rudimentary cellular structures have simple neural systems.

The human nervous system is the most complex neural system overall, with the majority of its components concentrated in the human brain. This system's working nature has allowed man to surpass all other creatures in a variety of qualities and abilities, including understanding, recognizing shapes and symbols, learning, speaking, remembering, perceiving, and precise control of the locomotor system (Afifi, 2018).

The field of technical advancement in artificial intelligence and information technology is one of the most significant areas that has been greatly impacted by the data of various technologies, which exceeds "our human ability to absorb and process information." There is no doubt that technology and its various means were invented to facilitate human life and functions in various fields, which cast a shadow on all aspects of daily life (Calum, 2016).

The field of artificial intelligence was founded just over 60 years ago, but during that time most of its accomplishments were modest. However, in 2012, when it was applied to the statistical fields of machine learning and deep learning, machines were able to perform speech recognition, image recognition, and natural language processing better than humans (Beheiry, 2019).

McCarthy used the phrase "artificial intelligence" in 1958 to describe the process of working toward improving machine intelligence to the point where it can either match or exceed human intelligence and be able to use logic to carry out jobs that humans might execute intelligently (Brigitte, 2018).

In order to understand the concept of artificial intelligence, it is first necessary to understand the concept of human intelligence. Human intelligence is defined as "the ability and skill to develop and find solutions to problems using symbols," different search techniques known as "knowledge," and the capacity to apply experience gained through "expertise" to derive new information and knowledge that leads to the development of solutions to problems in a particular field".

Each person has a particular amount of intellect, and human intelligence is what drives creativity and progress in the rise of many civilizations. Man has always been interested in studying the nature of human intelligence, how to quantify it, and creating computer programs to mimic its processes because of the significance of human intelligence (Bilal & Moussa, 2019).

For a long time, psychologists were the only scientists who studied human intelligence. However, in the last half of the 20th century, scientific advancements in all fields have led to the contribution and coherence of numerous sciences, including biology, physics, computers, philosophy, linguistics, physiological, and biological sciences, in the study and simulation of systems. The goal of studying human intelligence and development is to apply human experience and innate intelligence to computer programming systems for use in a variety of domains where a certain level of intelligence and experience is required to stay up to date with advancements in commercial, industrial, and agricultural applications (Abdel-Zahir, 2018).

Thus, the application of computers to the task of identifying various forms, symbols, and models gave rise to artificial intelligence systems. These systems were typified by the transfer of a portion of human intelligence techniques to computer programming systems, which in turn helped to create experience systems that incorporated a portion of human experience (Afifi, 2018).

According to this definition, artificial intelligence is "the science of creating computer devices and programs capable of thinking in the same way that the human brain works, learning as we learn, deciding as we decide, and acting as we act." It is one of the branches of computer science concerned with how machines simulate human behavior (Abdel-Wahab et al., 2018).

The ability of machines to behave in ways that are somewhat similar to those of humans is another prerequisite for artificial intelligence. This is achieved by applying AI techniques to work problems, and AI can offer creative solutions to a wide range of issues that arise in the workplace across a variety of industries (Abbas, 2020).

Artificial intelligence has been defined as: "that branch of computer science by which computer programs can be created and designed that simulate the style of human intelligence so that the computer can perform some tasks instead of humans, which require thinking, understanding, hearing, speaking and moving in a logical and organized manner." Following World War II, conventional programming systems gave way to computer programs that mimicked human intelligence in the form of games and puzzle solutions. These programs eventually led to the development of larger simulation systems, which eventually crystallized into artificial intelligence systems (Kazem & Hamid, 2020).

According to John McCarthy, who coined the term artificial intelligence in 1955 AD, it is also defined as "study and design smart systems that accommodate its environment and take measures that increase the chances of its success." Technical intelligence in this context refers to a person's ability to use modern technology to expedite work performance, improve performance across a range of fields, and—above all—accurately carry out tasks (Abdul Hadi, 2019). "Simulating human intelligence, and understanding its nature by making computer programs, capable of simulating intelligent human behavior" is another definition of artificial intelligence. Artificial intelligence is already present in many aspects of our lives, such as self-driving cars, drones, investment software, and many other applications (Majed, 2018).

The researcher defines artificial intelligence as follows: feelings, sensations, experiences, information, actions, and commands in the human mind that are implemented by machines and electronic systems that are relied upon in a simplified way to find appropriate solutions to various facts. These distinct definitions are despite the fact that they are the outcome of real and practical experiences.

***Artificial Intelligence Functions in Security Work***

Because of its versatility in military, industrial, economic, technical, medical, educational, and service applications, among other fields, artificial intelligence represents one of the Fourth Industrial Revolution's most significant outputs. It is also anticipated to lead to an endless stream of innovations. AI will be the driving force behind progress, growth, and prosperity in the coming years. Its innovations have the potential to create a new world that, while it may still seem far off in the future, current indications point to its imminent creation. This will usher in more industrial revolutions that will fundamentally alter human life, much like the tremendous and accelerating technological development and global transformations brought about by the fourth industrial revolution (Majid, 2018)

Artificial intelligence technologies are becoming more widely used. They have been incorporated into a variety of fields, such as criminal justice, health, and medicine. While this can be seen as a positive development for humankind, there are also worries that these technologies could pose a threat to human safety (Hawass, 2017).

*Using artificial intelligence tools to track traffic patterns:* Artificial intelligence is also used to analyze traffic patterns in order to accurately forecast and avoid collisions, as demonstrated by self-driving automobiles. Counterfeiting and fraud are combated using machine learning and artificial intelligence tools (WIPO, 2019).

*Using artificial intelligence to evaluate social networking data:* There are numerous artificial intelligence applications, including those employed by social networking sites to face bad phenomena, such as blocking extremist content on the Internet or attempting to prevent suicide through its website (Salmi, 2017).

As modern societies transition to a new stage of their social and economic growth, accompanied by new behavioral patterns supported by electronic information and data, security authorities are becoming more interested in using social analytics to analyze social network data to detect the possibility of riots and demonstrations in an area (Saleh, 2020).

Indeed, as the worldwide high-tech environment in which modern man lives develops, the world is heading toward a more dire and perilous state than we are currently experiencing. These days, the computer as the center of this environment is utilized not only in the domains of science and prediction, but in all human transactions and activities as a necessary component of modern technology (Bandaqa, 2020).

1. Using artificial intelligence methods to comprehend how accidents, related injuries, and fatalities are related:
   In order to comprehend the connection between accidents, the injuries that result from them, and fatalities, the IBM system was fed data from the New York City Police between 2013 and 2015. (Al -Hiti, 2020). These apps started to take over the industrial sector. They were successful in doing the mundane activities that people did in offices and factories, as well as jobs that humans were unable to complete, such exploring the depths of the ocean or space.
2. Using artificial intelligence techniques to learn about human behavior:
   Artificial intelligence programs have advanced to the point where they can now predict human interactions in the behavior recognition field. The Massachusetts Institute of Technology's AI Laboratory and Computer Science was created by an algorithm that examined over 600 hours of YouTube videos in order to study human behavior, and it has since become at 43% of test samples, the algorithm can then anticipate human behavior, which is less than 28% of human skill (Abd, 2020).

Artificial intelligence (AI) examines "big data," or the enormous volumes of personal and professional information that can be examined to spot changes in human behavior patterns and interactions. This complex data aids in developing a thorough understanding of societies and makes it easier to track trends in both individual and collective human behavior and forecast where it will go in the future.

***The Primary Obstacles and Cyber Threats***

The Internet network allowed researchers to access the various information resources that cover their scientific needs, circumventing issues and geographical and temporal obstacles. This made the Internet a true blessing and a new tool that reflects in its technical and scientific dimension a manifestation of this era. The Communications and Information Revolution played a significant role in the rapid and easy spread of information, turning the world from the various continents of the parties involved into a small village called a "cosmic village."

Although it is still viewed as a true blessing, the abundance of security risks, such as the potential for viruses to spread, hacking attempts, or intrusions that compromise device and user privacy, has turned the Internet into a curse that disturbs even the most affluent users when they use it. As a result, we shall highlight the key threats and issues associated with cyberspace:

*Electronic Piracy*

There is no doubt that the Internet represents the peak of human invention in the sphere of communications, information sharing, and availability in the current day; now, each of us can go to many nations throughout the world without leaving his home. All of the opportunities afforded by the network are not without drawbacks, which many users of this technology are unaware of.

The process of accessing global information resources on the Internet can enable hackers to trace all of the operations that the web service user has performed Nadim (2002), allowing them to tamper with their information and attempt to damage or distort it. Electronic piracy is an act analogous to the theft of a product from the shelves of some retailers, theft or distribution without authorization, or the use of content that has intellectual property rights. An American university was forced to pay a phone bill estimated at $200,000,

more than half of which was used for illegal communications. This phenomenon has spread to all countries in the world, with hackers able to access computers at the White House and the American Research Center (NASA) with only a computer and modem.

*Hacking*

The capacity to unlawfully access a particular target by taking advantage of security holes in the target's defense system is known as hacking in general. Here, the hacker is referred to as a "hacker" once the gadget is accessed. However, in this case, it is deemed a "cracker" when sabotage, deletion, theft, and breaching the privacy and confidentiality of information occur.

Therefore, hacking is the attempt by one or more individuals to gain access to any device or network associated with a particular field or area of study. This is done through the use of specialized programs designed to decode codes, crack passwords, and breach security barriers in order to identify the advantages and disadvantages of the device or information network that we are connected to. The term "hacking" was coined in the early 1960s to refer to brilliant programmers skilled in dealing with computers with high experience and accuracy by programming and designing the fastest and most accurate programs such as the Unix system, as opposed to the common meaning today, which is associated with the attribute of sabotage, an infringement on confidentiality and privacy, breaking firewalls, and so on. This is a typical mistake, the perpetrators of such criminal acts should have been referred to as 'crackers', a term borrowed from English that meaning breaking and smashing and refers to hackers who violently infiltrate operating systems with the goal of infiltration and sabotage. (Stang, 1996).

When discussing one or more computers within a single room, the task of securing data and information and preserving its integrity from interference and exposure to modification and alteration is relatively simple. However, when discussing computers connected to one another through multiple networks in various parts of the world, the situation becomes much more complex, and it can be declared that it is impossible due to the difficulty of determining or securing the path of information from its original origin to the desired goal.

*Viruses*

When the first computer viruses were reported in 1989, many people thought they were just a myth from science fiction stories, and the media and communication tried to solidify this belief in the minds of the general public. However, this phenomenon quickly transformed from a myth of scientific research stories into a real threat to the information revolution, which was powered by advanced and accelerated computer science technologies. It is a straightforward virus that causes harm and has the ability to alter and evolve into intelligent, creative viruses (Bashoush, 2002).

According to computer science, a virus is a tiny program or a portion of a program that attaches itself to other programs, alters their functionality, and then multiplies and spreads across the device. These are applications designed to inflict harm and take control of another computer, to cause mayhem and devastation, or to arouse strange pleasure.

*Malware Attack*

Malware is often introduced into a user's device through a variety of attack techniques, including social engineering. Users could be required to perform a task, like opening an attachment or clicking a link. Malware can also install itself without the user's knowledge or agreement by taking advantage of security holes in operating systems or browsers. Once

malware is installed, it can monitor user behavior, transmit private information to an attacker, help the perpetrator breach other network targets, and even make the user's device join a botnet that the attacker is using to further their malevolent goals. The following are some of the malware attacks:

1. Trojan virus: the user is tricked into thinking the file is dangerous. Trojan horses have the ability to penetrate systems and open a back door for attackers to use.
2. The ransomware program – barring the victim from accessing their data and threatening to destroy or expose it unless the ransom is paid. See our guide on preventing ransomware for more information.
3. "Magnified programs for the mop" – these programs write over the targeted files or wipe out the entire file system in an attempt to delete data or systems. Surfaces are typically used to cover up pirate activity following data leaks or to convey political messages.
4. Worms: These malicious programs are made to take advantage of openings in operating systems and flaws that allow unauthorized access. Following installation, the worm is capable of a variety of attacks, including as distributed denial of service (DDOS) rejection.
5. Spyware: These malicious applications give bad actors illegal access to data, including private data like credit card numbers and accreditation information. Mobile phones, desktop programs, and desktop browsers are all susceptible to spyware.

***Artificial Intelligence's Assistance to Solving Cyber Issues***

The issues associated with cybersecurity are growing as technology advances, particularly with the emergence of artificial intelligence. This is due to the possibility that artificial intelligence (AI) will both strengthen and complicate cyberattacks while simultaneously increasing the capacity to thwart them—a situation known as "double-edged swords."

Artificial intelligence techniques have the advantage of being able to interact positively with sophisticated cyber threats because these technologies, particularly those pertaining to data analysis, can aid in the identification of anomalous patterns and suspicious behaviors in cyber networks, thereby aiding in the early detection of potential attacks. By creating systems that automatically isolate compromised systems to stop assaults from spreading, autonomous response technologies can also be useful in lessening the impact of cyberattacks.

*Discover and Preventive Programs*

One of the most pressing issues in cybersecurity is the rapid creation of malicious applications. Artificial intelligence systems can scan enormous amounts of data, such as network traffic and system logs, to identify unusual patterns and situations that may suggest malicious software. Artificial intelligence systems can detect malicious programs and promptly prevent them from invading networks by continuously learning from new threats and attack technologies, thereby saving institutions from significant damage and loss (Abdu Ghani, 2020).

*User Behavior Analysis*

Institutions frequently struggle to detect internal risks and unauthorized activities in their networks. Artificial intelligence can play an important role in monitoring and analyzing user activity to detect anomalous actions. Artificial intelligence systems can detect suspicious acts, such as unauthorized access or data extraction, by identifying basic behaviors and comparing them to real-time data. This proactive approach enables organizations to detect and respond to possible hazards rapidly (Abdu Muttalib, 2019).

*Threat Intelligence and Prediction*

The cyber threat landscape is continually shifting, making it challenging for institutions to stay up. Artificial intelligence systems can collect and evaluate massive volumes of threat intelligence data from a variety of sources, including forums, the dark web, and cybersecurity reports. Artificial intelligence may produce important visions by recognizing patterns and connections in this data, allowing safety teams to respond to new dangers more proactively and strengthen their defenses (Al -Babli, 2019).

*Hunting and Fraud Discovery*

Fraud attacks remain a persistent problem, affecting both individuals and institutions. Artificial intelligence systems can successfully detect fake hunting attempts by analyzing email content, URL addresses, and user activity. Using automated learning approaches, artificial intelligence systems may adapt and increase their detection skills while attackers refine their tactics. This allows organizations to better defend their staff and systems, rather than falling victim to fraudulent hunting activities (Al Buhairi, 2019).

*Responding to Accidents and Automation*

When a security disaster happens, a quick response is critical to minimizing damage and reducing the time spent stopping activity. Artificial intelligence technologies can speed up accident response operations by automating typical activities including data collection, record analysis, and recognizing potential settlement indicators. By efficiently sorting and categorizing mishaps, artificial intelligence can improve cybersecurity teams' efficiency, allowing them to focus on the most complex and crucial duties (Khalifa, 2018).

To examine the overall influence of AI on cybersecurity, research reveals that the emergence of cyber risks and attacks has compelled organizations to implement AI-based technologies to defend their digital assets.

**Conclusion**

Artificial intelligence applications for security work are being developed, and it is envisaged that these applications will be used in the coming years to activate security decision-making, predict crimes, and strive to avoid them. As technology becomes more widely embraced within enterprises, the frequency of cyber threats and attacks increases. According to studies, there is an urgent need for safer methods to corporate cybersecurity that use AI-driven solutions to fight against ever-changing threats. Thus, the goal of this study was to evaluate the total impact of AI-based solutions on cybersecurity.

The study produced a number of findings, the most significant of which is that artificial intelligence is one of the fundamental axes, and that the advancement of science and the spread of information technology are helping to improve people's lives and integrate state building. There is also a great deal of attention being paid to creating smart systems that can act similarly. Simultaneously, the opposing current attempts to disrupt the atmosphere using the same methods, and dreams are wasted for clearly defined reasons and objectives.

Artificial intelligence has the potential to enhance cybersecurity by improving attack detection procedures, analyzing network behaviors, and creating smart security systems that can effectively respond to growing threats. Artificial intelligence can also be used to develop cyberattacks in more efficient and accurate ways, which can help identify unusual patterns and new threats more quickly. Finally, artificial intelligence can analyze large amounts of data

related to network activities and digital behaviors to anticipate and identify potential gaps and future attacks.

**References**

Abbas, A. (2020). Information Technology and Intellectual Property Rights Crime. Beirut, Lebanon: Arab Foundation for Science and Culture.

Abdel Hadi, Z. (2019). Artificial Intelligence and Expert Systems in Libraries. Cairo, Egypt: Dar Kitab for Publishing and Distribution.

Abdel-Muttalib, M. A. H. (2019). Intelligence Police: Police Work based on Artificial Intelligence and Information Analysis. Cairo, Egypt: Arab Renaissance House for Publishing and Distribution.

Abdel Wahab, S., Al-Ghitani, I., & Yahya, S. (2018). Opportunities and Threats of Artificial Intelligence in the Next Ten Years. Future Report. Supplement issued with the journal 'Trends of Events', Issue 27. Abu Dhabi, UAE: Future Center for Advanced Research and Studies.

Ahmed, H. A., NorZafir, M. S., Shaymah Ahmed, A.-Z., & Ahmad, K. (2022). Consumer Behaviour to Be Considered in Advertising: A Systematic Analysis and Future Agenda. Behavioral Sciences, 12(12), 472-493.

Alsharif, A. H., Salleh, N. Z. M., & Baharun, R. (2021a). The neural correlates of emotion in decision-making. International journal of academic research in business and social sciences, 11(7), 64-77.

Alsharif, A. H., Salleh, N. Z. M., & Baharun, R. (2021b). To better understand the role of emotional processes in decision-making. International Journal of Academic Research in Economics and Management Sciences, 10(2), 49-67.

Afifi, J. (2018). Artificial intelligence and expert systems. Cairo, Egypt: Al-Manhal for Publishing and Distribution.

Alsharif, A. H., Salleh, N. Z. M., Baharun, R., & Effandi, Y. M. (2021c). Consumer behaviour through neuromarketing approach. Journal of Contemporary Issues in Business and Government, 27(3), 344-354.

Al-Babli, A. Y. M. Z. (2019). The role of artificial intelligence systems in the prediction of crime. Police Thought Journal, 28(110), [Page numbers if available].

Al-Buhairi, A. S. J. M. H. H. (2019). The impact of artificial intelligence applications on raising the efficiency of security performance by applying road insurance (PhD thesis). College of Higher Studies, Police Academy, Cairo, Egypt.

Al Dhaheri, S. K. (2017). Artificial Intelligence 'New Competitive Power'. Future Support and Decision Support Center, Abu Dhabi Police, (299), Dubai, UAE: February Bulletin.

Al-Hiti, M. Y. (2020). The Role of Industrial Information Systems and Communications Technology in Industry Development. Amman, Jordan: Dar Ghaida for Publishing and Distribution.

Alsharif, A. H., Salleh, N. Z. M., Wan Amira, B. W. A., & Khraiwish, A. (2022). Biomedical Technology in Studying Consumers' Subconscious Behavior. International Journal of Online and Biomedical Engineering, 18(8), 98-114.

Alsharif, A. H., Salleh, N. Z. M., & Lina, P. (2023b). A Comprehensive Bibliometric Analysis of fNIRS and fMRI Technology in Neuromarketing. Scientific Annals of Economics and Business, 70(3), 1-14.

Al-Salmi, A. A. R. (2017). Information Technology. Amman, Jordan: Dar Al-Manajah for Publishing and Distribution.

Alsharif, A. H., Salleh, N. Z. M., Ahmad, K., & Lama, N. H. (2023a). Exploring the Path of Biomedical Technology in Consumer Neuroscience Research: A Comprehensive Bibliometric Analysis. International Journal of Online and Biomedical Engineering, 19(16), 127-144.

Battoush, K. (2002). The university library and the challenges of the digital technology revolution. Journal of Libraries and Information, 1(2), December.

Bandaqa, S. M. (2020). Using Augmented Reality Technology in Information Institutions. Alexandria, Egypt: Dar Al-Ma'rifat Al-Jami'ah.

Bilal, A. H., & Moses, A. (2019). Artificial Intelligence. Cairo, Egypt: Book Foundation for Publishing and Distribution.

Calum Chace (2016). The Economic Singularity: Artificial Intelligence and The Death of Capitalism. Tree Cs.

Darwish, S. A.-L. (2000). Communication Technology: Risks, Challenges, and Social Impacts (1st ed.). Cairo, Egypt: Egyptian Lebanese House.

Halsharif, A., Salleh, N., Md , & Baharun, R. (2020). Research trends of neuromarketing: A bibliometric analysis. Journal of Theoretical and Applied Information Technology, 98(15), 2948-2962.

Halsharif, A., Salleh, N. Z. M., & Baharun, R. (2021a). Neuromarketing: Marketing research in the new millennium. Neuroscience Research Notes, 4(3), 27-35.

Halsharif, A., Salleh, N. Z. M., & Baharun, R. (2021b). Neuromarketing: The popularity of the brain-imaging and physiological tools. Neuroscience Research Notes, 3(5), 13-22.

Hawas, M. A. (2017). Are we intentionally limiting urban planning and intelligence? a causal evaluative review and methodical redirection for intelligence systems. IEEE Access, 5, 13253-13259.

Halsharif, A. (2023). The Enhancing Islamic Advertising Effectiveness Through Emotional Processes and Consumer-Centric Elements. 2023 International Conference on Sustainable Islamic Business and Finance (SIBF), Bahrain. 5-11.

Kazem, Z. H., & Hamid, A. H. (2020). Strategy and Revolution of Information: The Secret of the Relationship Between Them 'Rooting, Analysis and Application'. Cairo, Egypt: Dar Al-Fajr for Publishing and Distribution.

Khalifa, I. (2018). Post-Information Society: The Impact of the Fourth Industrial Revolution on National Security. Future Books Series for Research and Advanced Studies. Cairo, Egypt: Arab Publishing and Distribution.

Majed, A. (2018). Artificial Intelligence in the United Arab Emirates. Department of Economic Studies and Policies, Ministry of Economy, Abu Dhabi, UAE: First Quarter Initiatives.

Nadim, A. (2002). Personal Privacy on: The Internet. Computer, Communications and Electronics Magazine, 19(2), 1-16.

Saleh, E. E. M. (2020). The Economics of Information Technology. Cairo, Egypt: Dar Al-Fikr Al-Jami'a.

Stang, D. (1996). Securite reseaux. Paris, France: Dunod.

WIPO. (2019). Trenders of the technology of the "artificial intelligence". [Description of the source].

Pileliene, L., Alsharif, A. H., & Alharbi, I. B. (2022). Scientometric analysis of scientific literature on neuromarketing tools in advertising. Baltic Journal of Economic Studies, 8(5), 1-12.

Yu, X., & Guo, H. (2019). A survey on IIoT security. IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS).

Y. Li, Q. Liu, (2021), A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Energy Reports, 7.

Lasry, B., & Kobayashi, H. (Eds.). (2018). Human decisions: thoughts on AI. United Nations Educational, Scientific and Cultural Organization.