Middle East Journal of
Scientific Publishing
Vol. (6) Issue (1)
Edition 18th
2023 (158 - 168)

THE USE OF ARTIFICIAL INTELLIGENCE IN DETECTING ELECTRONIC CRIMES

Razan Qassem Ali
College of Computer and Information Sciences, King Saud University, Riyadh, ***Saudi Arabia***
Mehmet Sabih Aksoy
College of Computer and Information Sciences, King Saud University, Riyadh, ***Saudi Arabia***

Published on: 6 Mar. 2023

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Abstract

With the increase in the use of phones and technological devices and the increase in their benefits, the rate of electronic crime has increased. Human capabilities are unable to confront and discover it directly and quickly, and it is not sufficient to address, investigate and solve it quickly. There is a need to improve the speed and performance of the methods of addressing these attacks to keep pace with electronic crimes. There is also an urgent need to develop electronic defense systems adaptable and flexible and have a high ability to detect threats periodically and quickly and strengthen the system to confront these attacks and overcome them in a smart way. In this work, the role and impact of artificial intelligence in detecting electronic crimes are addressed.

Keywords: Electronic Crime, Artificial Intelligence, Intelligent Crime Detection

* INTRODUCTION

The Internet and technology provide many opportunities and benefits in many areas such as society, medicine, science, and many other fields, but in return, it also opens the door to crimes for criminals [9]. These

operations increased dramatically, and impose threats to individuals, institutions, major companies, and global banks. With the passage of time and the development of technologies, human capabilities have become incapable of detecting threats and electronic crime. Thus, the role of artificial intelligence (AI) and its techniques in electronic warfare has emerged [8].

Traditional static algorithms are ineffective in the identification of threats, crimes and in combating electronic crimes. New methods such as comprehensive situational awareness, and highly automated responses to cyberattacks require extensive use of AI and knowledge-based tools [28]. The distributed and open architecture of cloud computing and services is becoming an attractive target for potential cyber-attacks by hackers, and AI-inspired computing methods are playing an increasingly important role in cybercrime detection and prevention through data mining and reasoning [19].

The purpose of this work is to explain what electronic crimes are and what their dangers are, how AI techniques have been applied to combat them, and the impact of AI based techniques in detecting electronic crimes.

* ELECTRONIC CRIME: DEFINITION AND PROBLEM

Electronic crime can be defined as crimes that can be committed by computers and technology. In general, it can be described as any crime committed by experienced computer users [20]. These crimes can take many forms, such as financial or scientific cybercrime, extortion, criminal, and other types [4]. The concept of fraud and theft has taken another ways with increased use of technology, such as theft of digital information, fraud through e-mail messages, sending viruses, and others [15] . With the advancement of technology and the many available to easy ways electronic, the level of electronic crime has increased and have diversified more and more [9].

Electronic crime can have several other names, such as "Cybercrime", " Internet Crimes"," Computer Crime", "Digital Crimes", " Network Crimes", or " Crimes of Information Technologies". It can be defined as a crime committed through electronic storage devices, computer systems, and networks, regardless of their terminology [20]. As technology

has become a tool for committing crimes, it enables criminals to commit many crimes. The level of crime ranges from easy to difficult, and from stealing personal information to stealing security information, or on a political and international level [17]. Cell phones, mobile devices, computers, processors, the Internet, and all telephone systems are vulnerable to criminal activities [9].

Electronic crimes take on several forms facilitated by the Internet, which are explained as follows:-

* **Electronic crime and intellectual property theft:** With the increasing occurrence of crimes using technology and the Internet, one of the most important crimes is the theft of intellectual property. The aim is to acquire proprietary products such as visual , photographic materials and other products or to acquire trade secrets such as market campaigns and other secrets, that help companies and institutions in their trade[5,34].

* **Blackmail, impersonation, and theft via the Internet:** Technology, the Internet, and social networks provide two sides of the same coin. The first is the benefits that help users carry out their banking, personal, and other operations. The other side provides a fertile environment for criminal activity such as piracy, information theft, and impersonation. These crimes represent a growing and major problem that is increasing in size day after day and represent a threat to society [7].

* **Economic espionage:** electronic crimes that facilitate economic espionage and theft are increasing. Economic espionage can be defined as companies collecting information and using it to increase their competitiveness with other competitors, increase productivity, and study what the user prefers in those companies. A distinction can be made between the terms economic espionage and competitive intelligence since the first is theft Information and the second is its conclusion from legitimate sources [26]. Economic espionage can be theft and misappropriation of documents, papers, and commercial secrets that belong to a specific category of beneficiaries, whether at the level of citizens of a country, This falls under the illegal use of property [9].

* **Computer intrusion:** it is Exposing the computer and its system to danger through several practices such as breaking security by doing several

practices and causing the computer to enter an unsafe state. Computer intrusions, reports of cyberstalking, and other computer-related crimes in which the computer is the main factor in the crime [20].

With the increase of digital data stored on a daily basis, processed on computers and multiple information to socialize more, share information, knowledge and shop and other practices using the Internet and computers. The barriers between countries, regions, and languages have been eliminated and the virtual world has become deeper than before [15]. Cybercrime has increased without knowing the perpetrator In fact [17], to reduce crimes, several precautions must be taken and threats must be discovered early. This is what AI can be used for. We will discuss this issue in the subsequent sections.

*** ARTIFICIAL INTELLIGENCE AND ELECTRONIC CRIME DETECTION**

The aim of using AI in cybercrimes is to find ways to solve complex problems and explore them before the crime occurs. It includes the methods that will make computers or machines work to simulate and analyze human behavior, such as reasoning, planning, thinking, etc. [28].

*** Application of Artificial Neural Networks**

Also called deep learning, it was founded in (1957) by Frank Rosenblatt [12]. It works on the union of sensory perception with other sensors to produce the creation of millions of neural networks [2]. Gou, X., & Jin, W., have deduced how the brain simulates processing where it does by interpreting or eliciting logic, learning things on its own, and then suggesting solutions [13].

Tyugu E., [28] proposed host-based intrusion detection through a neural network that recognizes patterns, detects, knows the output and recognizes patterns. Then compares patterns with logic and searches for similarities in the two types of patterns previously entered [28]. The detection of cyberattacks and cybercrime, which helps to reduce the damage to the system by means of accurate learning, is more productive because of the high speed in detecting intrusion and anomalies, as time plays a fundamental role in detecting attacks and intrusion attempts [9].

Neural networks or deep learning are used as Intrusion

Detection and Prevention Systems (IDPS) by detecting and preventing the infiltration of cybercrime [24]. The work is performed in two phases. In the training phase, ANN will learn the attacking techniques and the occupying factors according to what will be entered. The next phase is testing by connecting ANN to a network in use to produce outputs [27].

In the year (2009) IDS was proposed by Linda et al., based on a neural network that uses a specific integration of two algorithms, for the IDS-NNM algorithm has ability to capture all the experiences used for intrusion that are presented on the integrated network while generating any alerts that are not correct [18]. Also, in the same year a system based on artificial neural networks was designed to detect electronic exploratory attacks by Iftikhar et al. [1]. It is working on a feasibility examination to investigate potential attacks that could be a reason for more attacks in the network system. It was noted that the results depend on Multi-Layer Perceptron (MLP) and are more accurate and systematic [3].

*** Application of Expert Systems**

Dilek S. et al. developed an expert system in cybersecurity and electronic crime, on an anonymous base. The purpose was to collect data, develop variables, retrieve the stored data, and the last stage was implementation [9]. In the year (2014), an expert system called "OPENSKe" was invented, which is a program that works to analyze, identify, and match the level of threat related to transactions that exist on an e-commerce website, which led to providing a wide database and to analyzing expected threats to identify weaknesses [12].

Recently, attacks have been developed and classified based on wireless networks and the adoption of safety in their construction [23].

*** Application of Intelligent Agents**

Intelligent Agent (IA) is the recognition of movement using sensors, directs the entire activity to complete set objectives and actions using actuators [25]. One of the characteristics of the smart agent is flexibility in environments with the ability to move between them, this is implemented in those designated environments. Which makes it suitable for combating cybercrime due to its collaborative nature [11].

In (2006), Nogueira, J. implemented a system consisting of a

bootable state used to defend against cyberattacks and combined it with a multi-agent systems (MAS) approach and the ability to validate the characteristics of cyberattacks [21]. In the same year, Gou proposed another system consisting of several factors, and the purpose of it was to discover the computer worms to stop all hackers working to develop them [13], In (2013), Ganapathy, S. made a whole generation of worms disrupt the router which consumes a large amount of network transmission capacity [10].

In (2010) Kotenko et al. researched systems that advance multiagent protection against botnets and examined them for their overgrowth across the network are used to mitigate many cyberattacks [14]. Define the infrastructure and implementation features of these systems, examples of which are distributed denial-of-service attacks, vulnerability scans, and the sending of large numbers of spam messages [6].

*** CONCLUSION and FUTUR WORK**

The widespread development of technology, networks, and the use of electronic devices such as mobile phones, computers, social networks, and other technologies have a positive impact as they provided comfort and ease of access to information but may make many problems and electronic crimes that are difficult to manage by the human only, In this paper, we talk about the role and impact of AI in detecting and applying technologies in these crimes have been addressed.

A detailed explanation of the definition of cybercrime and how it occurs was mentioned, and then mentioned several problems of crimes, such as theft of personal information, plagiarism, and economic espionage. It is possible to apply some applications to protect the user from cybercrime by working and developing expert systems or neural networks that work with AI and defend.

The available academic resources and references provided us with many theories and frameworks and showed that AI technologies have many applications in detecting cybercrime. This paper reviews the role and impact of artificial intelligence in electronic crime and mentions the application of artificial intelligence and digital forensics in addition to giving the scope for future work.

The need for cybersecurity, awareness against electronic crime,

and potential attacks is increasing, which needs more study [9]. The environments of the institution's work require concentration on the network and the formation of environments to require agents of smart electronic sensors that work and detect potential attacks, counterfeiting, and other technologies Cyber-attacks [24].

When starting to apply the techniques and works of AI to impact electronic crime, we will need research and planning in the future. The challenges in this area revolve around the management of existing and mutated knowledge alongside the network and hierarchical and normative knowledge engineering in decision-making programs [16] future work on IDPS should be strengthened by a combination of technologies and algorithms that improve the performance of anomalous intrusion detection [9]. When it comes to IDPS, future work where IDPS are created should be strengthened by a combination of technologies and algorithms that improve the performance of anomalous intrusion detection [22].

There are some legal problems, such as due process, ethical issues, and issues related to authority or privacy, that exist due to the spread and branching of technology very quickly and its development.

*** REFERENCES**

Ahmad, Iftikhar ,Azween B. Abdullah,and Abdullah S.Alghamdi. "Application of artificial neural network in detection of DOS attacks."Proceedings of the 2nd international conference on Security of information and networks .2009 https://doi.org/10.1109/isiea.2009.5356382

Akbari, M., & Rahimi, Z. (2021). A comprehensive investigation of chitosan/tripolyphosphate nanoparticles using artificial neural networks. https://doi.org/10.21203/rs.3.rs-197903/v1

Al Hawawreh, M., Rawashdeh, A., & Alkasassbeh, M. (2018). An anomaly-based approach for ddos attack detection in cloud environment. International Journal of Computer Applications in Technology, 57(4), 312. https://doi.org/10.1504/ijcat.2018.10014729

Ayyoub, H. Y., AlAhmad, A. A., Al-Serhan, A., Al-Abdallat, M. F., AlMuheisen, E., Boshmaf, H., Abu-Taleb, Y. A., Alqudah, Y. O., & Alshamaileh, Y. (2022). Awareness of electronic crimes related to elearning among students at the University of Jordan. Heliyon, 8(10). https://doi.org/10.1016/j.heliyon.2022.e10897

Blaskovic, A. K., Rusk, J.-D., Parker, V. C., & Payne, B. R. (2022). Cybercrime and intellectual property theft: An analysis of modern digital forensics. Proceedings of the Future Technologies Conference (FTC) 2022, Volume 2, 536–542. https://doi.org/10.1007/978-3-031-18458- 1_36

D., A., K.A., V. K., S., S. C., & P., V. (2019). Malware traffic classification using principal component analysis and Artificial Neural Network for extreme surveillance. Computer Communications, 147, 50– 57. https://doi.org/10.1016/j.comcom.2019.08.003

Deora, R. S., & Chudasama, D. (2020). Brief Study of Cybercrime on an Internet. Cybercrime and Society, 1–20. https://doi.org/10.4135/9781446212196.n1

Derfouf, M., & Eleuldj, M. (2017). Performance analysis of intrusion detection systems in the cloud computing. 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), 1–6. https://doi.org/10.1109/cloudtech.2017.8284716

Dilek, S., Cakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to Combating Cyber Crimes: A Review. International Journal of Artificial Intelligence & Applications, 6(1), 21– 39. https://doi.org/10.5121/ijaia.2015.6102

Ganapathy, S., Kulothungan, K., Muthurajkumar, S., Vijayalakshmi, M., Yogesh, P., & Kannan, A. (2013). Intelligent feature selection and classification techniques for intrusion detection in networks: A survey. EURASIP Journal on Wireless Communications and Networking, 2013(1).

https://doi.org/10.1186/1687-1499-2013-271

Gandhi, K. (2011). An Overview Study on Cyber crimes in Internet. Gandhi, 395–428. https://doi.org/10.1201/b10718-26

Georgieva, T., & Petkov, P. (2018). Expert framework for measuring the institutional capabilities to counter hybrid threats: Empirical Data Analysis. Information & Security: An International Journal, 39(3), 237–256. https://doi.org/10.11610/isij.3920

Gou, X., & Jin, W. (2012). Multi-agent system for security auditing and worm containment in metropolitan area networks. Proceedings Autonomous Decentralized Systems, 2005. ISADS 2005. https://doi.org/10.1109/isads.2005.1452052

Kotenko, A. Konovalov, A. Shorov, Agent-based modeling and simulation of botnets and botnet defence, in: Proc. Conference on Cyber Conflict, CCD COE Publications, Tallinn, Estonia, 2010

Jarrett, A., & Choo, K. K. R. (2021). The impact of automation and artificial intelligence on Digital Forensics. WIREs Forensic Science, 3(6). https://doi.org/10.1002/wfs2.1418

Jeyanthi, S., Maheswari, N. U., & Venkatesh, R. (2012). Implementation of biometrics based security system with integrated techniques. Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology. https://doi.org/10.1145/2393216.2393223

Kant, N. (2022). How cyber threat intelligence (CTI) ensures cyber resilience using artificial intelligence and Machine Learning. Methods, Implementation, and Application of Cyber Security Intelligence and Analytics, 65–96. https://doi.org/10.4018/978-1-6684-3991-3.ch005

Linda, O., Vollmer, T., & Manic, M. (2009). Neural network based Intrusion Detection System for critical infrastructures. 2009

International Joint Conference on Neural Networks. https:/ /doi.org/10.1 109/ijcnn.2009.5 17 8 59 2

Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. Annual Review of Criminology, 2(1), 191–216. https://doi.org/10.1146/annurev -criminol-032317-092057

Monteiro, A. C., França, R. P., Arthur, R., & Iano, Y. (2021). An overview of Explainable Artificial Intelligence (XAI) from a modern perspective. Explainable Artificial Intelligence for Smart Cities, 1–11. https://doi.org/10.1201/9781003 172772-1

Nogueira, J. (2006). Mobile intelligent agents to fight cyber intrusions. The International Journal of Forensic Computer Science, 28–32. https://doi.org/10.5769/j200601 003

Jabez, J., & Muthukumar, B. (2015). Intrusion detection system (IDS): Anomaly detection using outlier detection approach. Procedia Computer Science, 48, 338–346. https://doi.org/10.1016/j.procs.2 015.04.191

Shafi, Q. (2012). Cyber Physical Systems Security: A brief survey. 2012 12th International Conference on Computational Science and Its Applications. https://doi.org/10.1109/iccsa.20 12.36 Jen, C. T., Hu, J., Zheng, J., & Xiao, L. L. (2019). The impacts of corporate governance mechanisms on knowledge sharing and supply chain performance.

International Journal of Logistics Research and Applications, 23(4), 337– 353. https://doi.org/10.1080/1367556 7.2019.1691515

Sharma, M. (2017). Digital data stealing from ATM using data skimmers: Challenge to the forensic examiner. Journal of Forensic Sciences & Criminal Investigation, 1(4). https://doi.org/10.19080/jfsci.20 17.01.555567

Shi, Y. (2019). The impact of artificial intelligence on the accounting industry. Advances in Intelligent Systems and Computing, 971–978.

https://doi.org/10.1007/978-3-030-15235-2_129

Snyder, H., & Crescenzi, A. (2017). Intellectual capital and economic espionage: New crimes and new protections. Transnational Financial Crime, 433–442. https://doi.org/10.4324/9781315084572-24

Subba, B., Biswas, S., & Karmakar, S. (2016). A neural network based system for intrusion detection and attack classification. 2016 Twenty Second National Conference on Communication (NCC). https://doi.org/10.1109/ncc.2016.7561088

Tyugu, E. (2020). Artificial Intelligence and defense issues. Artificial Intelligence, Cybersecurity and Cyber Defense, 105–186. https://doi.org/10.1002/9781119788195.