APPLICATIONS OF ARTIFICIAL INTELLIGENCE FOR CRYPTOGRAPHIC AND SECURITY PURPOSES

Cristian CRETU[1*], Daniil SCHIPSCHI[1], Marin NEGAI[1]

[1]Department of Software Engineering and Automation, group FAF-223, Faculty of Computers, Informatics, and Microelectronics, Technical University of Moldova, Chișinău, Republic of Moldova

**Corresponding author: Cristian Cretu, cristian.cretu@isa.utm.md*

***Abstract**:The use of artificial intelligence (AI) in cryptography and security is a rapidly growing field. In security, AI is used to detect potential threats and weaknesses within a system by identifying "safe" versus "malicious" behaviors. AI security tools are able to process large amounts of data and create activity profiles that can reveal malicious behavior, mimicking the threat-detection capability of human analysts. AI is also used to automate tasks, prioritize alerts, predict breach risks, and respond to security incidents. In cryptography, AI is used to develop and improve existing encryption algorithms. However, the use of AI in cybersecurity is not without its challenges. As AI becomes more widely used in the cybersecurity field, companies need to take precautions to protect themselves from potential adverse effects. Hackers can try to exploit security algorithms by targeting the AI system itself. The use of AI in cybersecurity creates a dilemma known as the "AI/cybersecurity conundrum," where AI can be used for both good and bad purposes.*

***Keywords**: machine learning, protection, hash algorithms, malice, safety*

Introduction

Today artificial intelligence has started to be used for various needs, this being a revolutionary technology. Of course there are many implementations of AI, but this article will focus on the applications of AI in cryptography and security. It plays an increasingly important role in the development of encryption algorithms and methods of analysis and improvement of cyber security. The development of these domains, in turn, being essential for the security of users' personal data.

Concept definition

In the following lines we will provide an overview of AI and some terms in the field for a better understanding of the article.

Artificial Intelligence - (referred to hereafter by its nickname, “AI”) is the subfield of Computer Science devoted to developing programs that enable computers to display behavior that can (broadly) be characterized as intelligent. Most research in AI is devoted to fairly narrow applications, such as planning or speech-to-speech translation in limited, well defined task domains. But substantial interest remains in the long-range goal of building generally intelligent, autonomous agents, even if the goal of fully human-like intelligence is elusive and is seldom pursued explicitly and as such [1].

Cryptography **-** is the practice and study of techniques for secure communication in the presence of adversarial behavior. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, information security, electrical engineering, digital signal processing, physics, and others [2].

Machine learning **-** uses statistical techniques to give computer systems the ability to “learn” (e.g., progressively improve performance) using data rather than being explicitly programmed. Machine learning works best when aimed at a specific task rather than a wide-ranging mission [3].

Deep learning - is part of a broader family of machine learning methods based on learning data representations, as opposed to task-specific algorithms. Today, image recognition via deep learning is often better than humans, with a variety of applications such as autonomous vehicles, scan analyses, and medical diagnoses [4].

In order to gain a more comprehensive understanding of artificial intelligence and its applications in cryptography and cyber security, we will break down this article into two distinct sub-sections. The first portion will focus on security, exploring how AI can be used to detect potential threats and weaknesses within a system. The second part will delve into cryptography, investigating how AI can be employed to develop and improve existing encryption algorithms.

Application of AI in security

AI security solutions are programmed to identify "safe" versus "malicious" behaviors, by cross-referencing user activity across an environment and comparing it to similar environments. This process, known as "unsupervised learning," allows the system to independently create patterns. For more complex AI platforms, "deep learning" is used to detect malicious behavior.

AI cybersecurity tools have the ability to process and assess vast amounts of data, enabling them to create activity profiles that might reveal malicious behavior. This mimics the threat-detection aptitude of human analysts. In addition, AI can be used for automation, grouping alerts, classifying warnings, automating reactions, and more. It is often employed to enhance the work of first-level analysts [5].

AI is not just a broad, generic approach to strengthen security in various sectors. It is a tool that can help improve the efficiency of teams and departments. Benefits include:

- *IT Asset Inventory* - the process of gathering a comprehensive and precise list of all users, applications, and devices with any connection to information systems. Additionally, categorizing and evaluating the importance of the assets to the business is also essential [6].
- *Threat Exposure* - the potential vulnerability of an organization to cyber attacks that are currently fashionable among hackers. AI-based cybersecurity systems can detect and analyze these global and industry-specific threats and provide insights to help organizations prioritize their security measures and protect themselves from the most likely attacks [6].
- *Controls Effectiveness* - it is important to understand the impact of the various security tools and security processes that you have employed to maintain a strong security posture. AI can help understand where your infosec program has strengths, and where it has gaps [6].
- *Breach Risk Prediction* - AI-based systems can utilize IT asset inventory, threat exposure, and control effectiveness data to forecast where and how your organization is most likely to be breached. This prediction can help you plan for resource and tool allocation towards areas of weakness, and use AI-derived insights to configure and enhance controls and processes to better protect your cyber resilience [6].
- *Incident response* - the process of using AI powered systems to prioritize and respond to security alerts quickly, as well as identify underlying causes of security incidents to prevent future problems [6].
- IT security professionals can leverage AI and machine learning to implement good cybersecurity measures and reduce the opportunity for malicious activity. Unfortunately, state-sponsored attackers, criminal organizations, and ideological hackers can also use AI to bypass security measures and go undetected. This creates a difficult dilemma for cybersecurity professionals known as the "AI/cybersecurity conundrum."

As AI advances and is more widely used in the cybersecurity field, companies should take precautions to protect themselves from any potential adverse effects of this innovative technology [4].

- Machine learning and artificial intelligence can be used as a form of defense against cyber-attacks, however, hackers can try to exploit security algorithms by targeting the data used to train them and the warning flags they search for [4].
- Cyber criminals can take advantage of AI to breach security measures and create malicious software that modifies its form to stay undetected [4].

- AI systems will produce unreliable outcomes and false alarms if not provided with a large amount of data and occurrences [4].
- If data manipulation is not detected, organizations will have difficulty retrieving the accurate data that powers their AI systems, which could have catastrophic results [4].

Another application of the Artificial Intelligence would be steganography. Steganography is an important technique used in the field of security and cryptography to conceal sensitive information within seemingly harmless data. However, steganography poses a significant challenge for traditional security systems, as it is difficult to detect without prior knowledge of where to look. This is where the use of AI can prove to be highly beneficial. With its ability to recognize patterns and anomalies within complex data, AI algorithms can be trained to analyze digital files, such as images or audio files, and detect any irregularities in the data that may indicate the presence of hidden information. By identifying such patterns, AI can flag files that are likely to contain steganographic content, thus enhancing the effectiveness of traditional security measures.

AI algorithms can be trained to analyze digital files, such as images or audio files, and detect any irregularities in the data that may indicate the presence of hidden information. For example, an AI algorithm may identify unusual patterns or inconsistencies in the pixel values of an image that may indicate the presence of hidden information. By comparing the analyzed data against a baseline of expected results, AI can flag files that are likely to contain steganographic content. Moreover, AI can also be used to develop new steganographic techniques that are more difficult to detect. By analyzing large datasets and identifying patterns in the data, AI can provide insights into new approaches and techniques for hiding data within files that are more resistant to detection. This can be useful for both defenders and attackers in the ongoing cat-and-mouse game of steganography detection.

However, the use of AI in steganography detection is not without its challenges. For example, attackers may use AI to develop new and more sophisticated steganographic techniques that are more difficult to detect by traditional security systems. Moreover, there are also concerns about the potential for false positives, where AI algorithms may flag innocent files as containing steganographic content. To address these challenges, it is important to develop AI algorithms that are both accurate and reliable in detecting steganography.

Application of AI in cryptography

The advantages of AI relies on its ability to recognize patterns and regularities within complex data. On the other hand, cryptography has the aim to maximize diffusion and chaos in the ciphertext and avoid any possible patterns that may lead to the discovery of the encryption algorithm [3].

It is required that the ciphertext is a complex randomized representation of a plaintext usually associated with the application of a one-way function which has no inverse solution. Since cryptography relies on encoding some message using a randomly generated field of numbers, we can give the AI some initial inputs and train it to recognize or identify some vulnerabilities in the algorithm or the encrypted data [3].

This way, AI can be used to test the encryption algorithm and find weaknesses within it before using it for a real purpose. But there remains one question, brought up by Leslie Valiant and Michael Kearns in their article, about the inefficiency and helplessness of artificial intelligence when dealing with breaking secure cryptographical algorithms [7].

There are limitations on learning Boolean formulae and finite automata due to multiple reasons, as:

- *Computational complexity*: since the algorithms of encryption and decryption are very complex, even if there would be a polynomial-time learning algorithm, it could take too long to run and become impractical to implement even on powerful computers.
- *Information-theoretic security*: the encrypted data should not reveal any clues about the input or the nature of the algorithm.

- *Randomness*: cryptographical algorithms and protocols use randomness to encrypt data, which makes it very difficult to decrypt something without knowing the secret inputs or functions used in the protocol.
- *Cryptographic primitives*: cryptographic protocols use different approaches, such as one-way functions, hashing algorithms, symmetric or asymmetric encryption, which provide strong privacy and security.

This means that even if we could construct an AI model able to decipher, for example, RSA algorithm with unknown private key, it would take a lot of time to train and learn the way to decipher it, that would make its' purpose irrelevant.

That implies that the advantages of Machine Learning cannot be used efficiently on this kind of algorithms or protocols, even if we give the system some restraints that would help to learn to break the RSA algorithm. It appears that Artificial Intelligence is not convenient for trying to "break" cryptographic algorithms, but it proves itself a useful and powerful tool in testing them and avoiding weaknesses and repetitive patterns in the ciphertext. AI can be also used for faster generation of encryption keys, as it can simulate different models and make a decision based on the outcome of these simulations. However, this order may change with the development of quantum computers that would make breaking RSA much easier and could mark the end of the prime number - based encryption.

Conclusions

In conclusion, the use of Artificial Intelligence (AI) in cryptography and security is rapidly increasing in importance. The AI security solutions are capable of identifying and analyzing vast amounts of data to detect malicious behavior, as well as provide valuable insights to improve the overall security posture of an organization. As cyber threats continue to evolve and become more sophisticated, AI has become a critical tool in the fight against these threats. The applications of AI in security include IT asset inventory, threat exposure analysis, breach risk prediction, and incident response. However, it is important to note that as AI advances and becomes more widely used in the field, organizations must take the necessary precautions to protect themselves from the potential negative effects of this innovative technology and invest in its' development for their own protection. Additionally, the use of AI in cryptography can help in developing and improving existing encryption algorithms, making the secure communication of private messages more robust. As this technology continues to advance, it is likely that we will see new and innovative applications for it in security and cryptography.

References:

1. RICHMOND T., Logic and Artificial Intelligence.[Online] [Accessed on 08.03.2023] Available: https://plato.stanford.edu/entries/logic-ai/
2. RIVEST R. L. (1990). "Cryptography". In J. Van Leeuwen (ed.). Handbook of Theoretical Computer Science. Vol. 1. Elsevier [Online] [Accessed on 07.03.2023] Available: https://people.csail.mit.edu/rivest/pubs/Riv90a.pdf
3. BLACKLEDGE J., Applications of Artificial Intelligence to Cryptography. [Online] [Accessed on 07.03.2023] Available: https://arrow.tudublin.ie/cgi/viewcontent.cgi?article=1250&context=engscheleart2
4. Using Artificial Intelligence in Cybersecurity. [Online] [Accessed on 10.03.2023] Available: https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity
5. What is AI Security? [Online] [Accessed on 10.03.2023] Available: https://www.vectra.ai/learning/ai-security
6. What is AI for security? [Online] [Accessed on 08.03.2023] Available: https://www.servicenow.com/uk/products/security-operations/what-is-ai-security.html
7. KEARNS M., VALIANT L.,Cryptographic Limitations on Learning Boolean Formulae and Finite Automata [Online] [Accessed on 09.03.2023] Available: https://www.cis.upenn.edu/~mkearns/papers/crypto.pdf