AI for Security of Distributed Systems

MAREK R. OGIELA, URSZULA OGIELA
AGH University of Krakow,
30 Mickiewicza Ave, 30-059 Krakow,
POLAND

Abstract: - Cryptographic techniques are currently used in computer security systems designed to guarantee the integrity and security of encrypted information. They are based on advanced cryptographic algorithms that can also operate on a public key infrastructure. Such algorithms can also be based on user keys and personalized approaches applied to encrypt data and create VPN tunnels. The paper will present new possibilities of using artificial intelligence algorithms in the creation of new protocols designed to guarantee the cybersecurity of distributed computer systems. Artificial intelligence techniques can find application in such an area, especially in the analysis of protocol security, and can also be applied to the creation of new protocols dedicated to specific remote services, which will provide a greater level of security and allow better data protection.

Key-Words: - Cybersecurity, Artificial Intelligence, cryptographic protocols, cognitive cryptography, security protocols, user-oriented steganography.

Received: February 18, 2024. Revised: August 13, 2024. Accepted: September 9, 2024. Published: October 21, 2024.

1 Introduction

Computer systems security procedures are extremely important with regard to the data processed and services performed remotely by computer systems. This is caused due to the increasing sizes of data being transferred and the need for frequent information access protected in online services, [1]. The development of IT security protocols is one of the most important in advanced computing technologies, in which applications are worldwide and allow the acquisition, storage, and processing of huge amounts of data generated by users of networks and IoT sensors. As a result, newer and newer solutions are being proposed to ensure the confidentiality of transmitted IoT data. These solutions need to be constantly improved and take into consideration different factors, like the personalization of developed solutions, increasing number of cryptanalysis approaches and attacks, which can be performed by hackers or bots. One of the most important directions of development of advanced techniques for computer system security is the creation of solutions that use personal characteristics of users or meaning description of secret o data. Such protocols define a new area of advanced and contemporary cryptography, which is called cognitive cryptography, [2].

The result of using such procedures may be the greater application of artificial intelligence (AI) solutions in the creation of secure and efficient cryptographic algorithms. The subject of this work will therefore be ways of applying AI methods, as well as cognitive reasoning procedures in the creation of cybersecurity solutions. Among the many applications, the most interesting seems to be finding answers to the following questions:

- Can AI help to create personalized keys and secure transmission protocols?
- Can AI affect the proper functioning of cryptographic protocols?
- Can AI detect vulnerabilities in computer system security?
- Can information read by attackers be encrypted using AI in such a manner that it cannot be understood even after decoding?

In the following sections of this work, the methods and possibilities of using artificial intelligence techniques to develop safe and effective algorithmic solutions, the purpose of which will be to ensure the integrity and confidentiality of transmitted information, will be discussed. New secure protocols for authenticating websites and computer systems will also be presented.

2 Security Protocols using AI

One of the first applications of AI in cybersecurity is the definition of user-oriented, efficient, and personalized cryptographic algorithms. Among the great number of application areas of artificial intelligence, it is worth noting the possibility of using AI algorithms to determine personal biometric features or behavioral traits, which as unique parameters uniquely describe a given user. Such features can therefore be used to generate special cryptographic keys and steganographic algorithms for secrets concealing, in which personal factors will determine the way data is distributed.

Artificial intelligence algorithms used in such applications allow for the selection of unique representative features characterizing a specific participant of the protocol. In such a case, known AI techniques based mainly on artificial neural networks or pattern recognition methods can be effectively used to determine the most representative personal features, [3], [4], [5]. Of course, artificial intelligence methods allow for the determination of several independent vectors of characteristics, because they operate on much larger records of personal features, which contain several personal characteristics having the form of biometric traits, behavioral features, or medical information. Training an appropriate classifier to select the set of best traits for a given participant, can be performed with the application of supervised machine learning methods, [6].

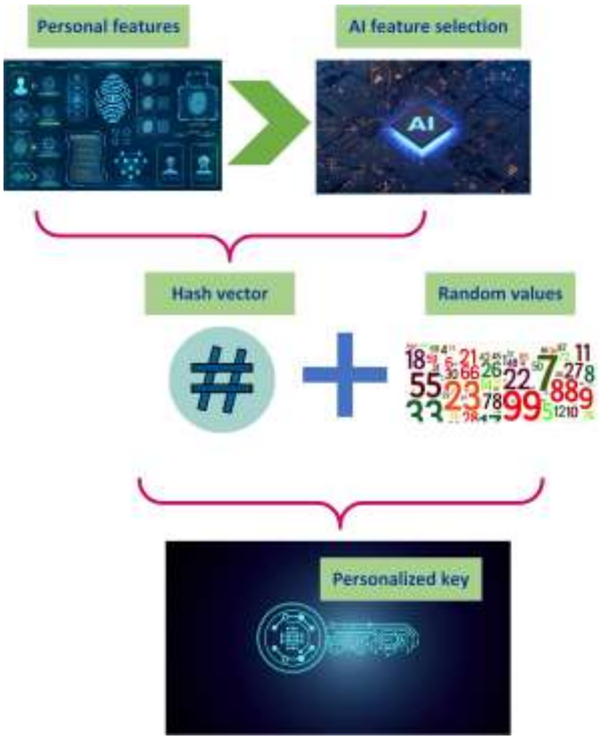

Fig. 1: User-oriented security key generation using artificial intelligence methods (own development)

After defining a set of personal features for a given participant, it will be possible to use it in cryptographic and steganographic procedures. One of the most important possible applications is generating user-oriented cryptographic keys and authorization codes for participants (Figure 1). For the creation of such keys or codes, it is necessary to generate a personalized vector containing selected user traits, with the application of a hash function, allowing one to obtain a key of a specified length. For those generated in this way, in the next step, it is necessary to add random bit sequences, which allow that the keys to have the necessary bit length depending on the types of cryptosystems, i.e. symmetric or asymmetric cryptographic procedures.

It is worth emphasizing that the procedure for the creation of personalized keys is a general procedure and also allows for the creation of sets of keys, which will belong to one particular user. Besides the use of computational intelligence algorithms to generate personalized keys, such algorithms can also be useful for creating secure user authentication, and authorization protocols. An example of such an application can be CAPTCHA authentication codes, which have the form of pictures or thematic questions related to user experiences. In such protocols, artificial intelligence algorithms allow for the generation of appropriate sets of patterns directly related to the expertise area or knowledge possessed by a specific user. They also allow for the generation of required sets of questions focused on the knowledge or experiences of the participants of the protocols.

Another very important application of personal characteristic vectors, previously determined by artificial intelligence algorithms for a specific participant of the protocol, is the application of such vectors as keys for secret information distribution in digital containers. Such data-hiding procedures will enable placing information in a way that depends on the owner of the key used to disperse data in the container. Similarly, to encryption keys, also in information hiding tasks, for one participant, there may be created several personalized keys for hiding data. This provides additional possibilities for placing several different secrets in one container so that each of them is placed in a different manner, with the application of different personal keys.

For the presented procedures, the issues of their security are also important. Analyzing the resistance of the presented methods to cryptographic attacks, it can be seen that these protocols are computationally safe and guarantee strong security. This is mainly due to the application of various personal features in the creation of encryption and information-hiding keys, as well as their extension with random bit sequences. Security also results from a random selection of sets of patterns used in authentication procedures, as well as randomness in the distribution of secrets on data carriers. For such solutions, an effective cryptanalytic attack is a brute force attack.

3 User-Oriented Locking Protocol

In this section will be presented a new AI-based locking schema that can provide a high security level to encrypted data, by leveraging the ability to join the meaning of encrypted data with personalized vectors.

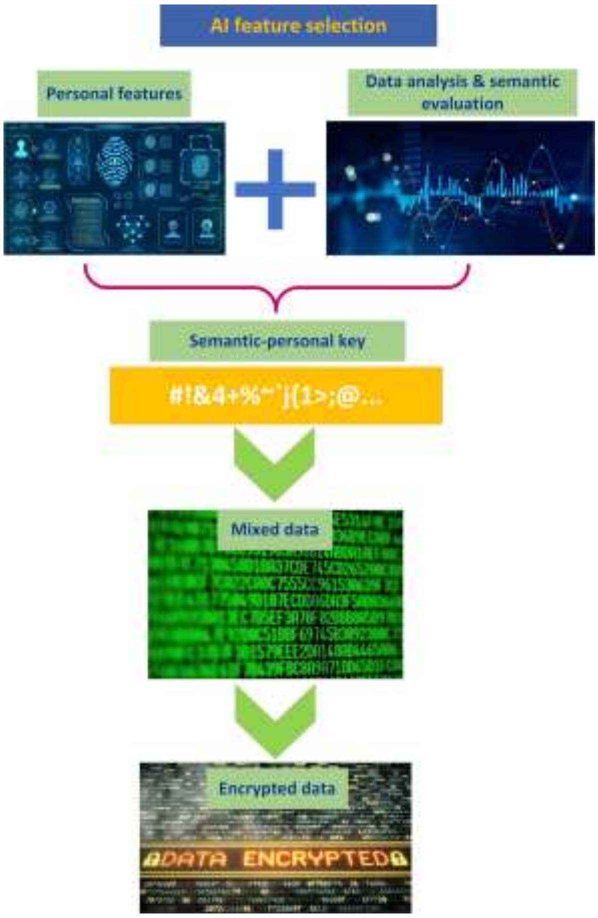

Fig. 2: Locking protocol based on AI methods (own development)

To define a protocol that allows for the introduction of an additional level of data security, which will allow them to function safely even when the encryption routine is broken, it is obligatory to use artificial intelligence techniques. Such protocols may be defined in the following manner (Figure 2):

- Information intended for encryption or concealment is analyzed using artificial intelligence methods to determine its content. As a result of such analysis, a semantic description vector can be obtained that uniquely describes this data, [7].
- A personal feature vector is also determined for encrypted or concealed data, which can be dependent on the sender or recipient of this data.
- Semantic and personalized feature vectors, will be used to disperse data using the created semantic-personal key.
- The shuffled input data is then encrypted with the application of selected encryption or concealment procedure.
- The hidden or encrypted data is securely stored in databases or sent to other participants or locations.
- In order to recreate the data, it is obligatory to decrypt it and restore using the original key.
- At the end the decrypted data can be read using the semantic-personal key.

The presented protocol is characterized by resistance to known cryptanalytic attacks in terms of security. When the man-in-the-middle attack is performed, even if the encryption key is revealed, it will only allow decryption of the dispersed data, which causes that the information will still be secure and unreadable as a result of shuffling them with a semantic-personal key, which depends on the semantic content of the information or participants of the protocol.

When a brute force attack is conducted, it is possible to decrypt the shuffled data, but it requires a high time complexity. Decrypting the data without any knowledge of the semantic or personal keys seems to be impossible due to their random characteristics. The cryptanalysis task of such methods also requires checking that the reconstructed information has the correct semantic (dictionary) meaning, and this is almost impossible when conducting a brute-force approach.

4 Polymorphic Keys Generation

The last example of the application of AI methods for security purposes is the generation of polymorphic encryption keys.

Polymorphic keys are such keys that can be transformed into various forms and where every form of the key will allow to deciphering other data. Upon transformation of the polymorphic key to another form, another input secret is decoded from the encrypted data. Such keys will have such a property that they will depend on a number of various encrypted input data. While deciphering by means of such keys, depending on the current form, it will be possible to decode a different secret or another part of a larger secret divided into a number of various parts.

Application of AI methods for the generation of such keys may also refer to the methods of transformation of such keys to various forms so that it is not easy for execution by third persons, should they obtain even one of the possible key forms. The key transformation algorithm will depend on parameters related to a given user or a group of protocol participants, who together can use such polymorphic keys.

A generation of polymorphic keys can be run with the use of AI approaches and some independent encryption keys meant for the concealment of various data, which will subsequently be combined into one entirety and mixed appropriately. In this case, decoding individual secrets will depend on the extraction procedure from the mixed key of every single independent key.

There is a slightly different approach to generating polymorphic keys, that is the application of threshold division procedures [8], [9]. Such procedures make it possible to generate various component shares and they frequently allow thedivision various input data. In this case, the input data could be the independent keys, which at the stage of application of the threshold scheme will enable, depending on the configuration of the shares put together, to re-create another independent key and to use it to decrypt the information.

5 Conclusions

This paper presents methods of using advanced artificial intelligence algorithms in the creation of new, effective, and secure protocols that guarantee the security of information and computer infrastructure. The described methods also allow to prevent cyberattacks on computer systems. Currently, issues related to cybersecurity are very important, mainly due to the huge number of Internet users and multimedia services. This affects global digitalization in the field of communication and the increasing volume of data transmissions, [10], [11].

In this work, we tried to present the main areas of using computational intelligence algorithms for applications in modern cryptography. It was therefore presented how such algorithms may have an influence on the development of new branches of cybersecurity, especially such areas as user-oriented cryptography and cognitive cryptography. It also discussed how artificial intelligence techniques can prevent attacks and incidents related to users' credentials leakage or unauthorized access.

This paper also discusses methods of creating secure cryptographic protocols based on semantic-personal keys created using artificial intelligence algorithms.

References:

[1] Ogiela, M.R. Ogiela, L.: AI-Based Cybersecurity Systems, Lecture Notes on Data Engineering and Communications Technologies, Vol. 202, 2024, pp. 166–173, https://doi.org/10.1007/978-3-031-57916-5_15.

[2] Ferguson, N., Schneier, B.: *Practical Cryptography,* Wiley, 2003.

[3] Albus, J.S.: The engineering of mind, *Information Sciences,* Vol. 117, No. 1–2, pp. 1-18, 1999.

[4] Bermúdez, J.L.: *Cognitive Science*, Cambridge University Press, 2022.

[5] Perconti, P., Plebe, A.: Deep learning and cognitive science, *Cognition,* Vol. 203, 104365, 2020, DOI: 10.1016/j.cognition.2020.104365.

[6] Zhang, H., Liu, F., Li, B., Zhang, L., Zhu, Y., Wang, Z.: Deep discriminative image feature learning for cross-modal semantics understanding, *Knowledge-Based Systems,* Vol. 216, 106812, 2021, DOI: 10.1016/j.knosys.2021.106812.

[7] Weiland, L., Hulpuş, I., Ponzetto, S.P., Effelsberg, W., Dietz, L.: Knowledge-rich image gist understanding beyond literal meaning, *Data & Knowledge Engineering,* Vol. 117, 2018, pp. 114-132.

[8] Tang, S.: Simple Secret Sharing and Threshold RSA Signature Schemes. *Journal of Information and Computational Science*, Vol. 1, No. 2, 2004, pp. 259-262.

[9] De Santis, A., Masucci, B.: New Results on Distributed Secret Sharing Protocols. *Lecture Notes in Computer Science*, Vol 13942. Springer, Cham, 2023.

[10] Premadasa, H.K.S., Meegama, R.G.N.: Extensive compression of text messages in interactive mobile communication, *2013 International Conference on Advances in ICT for Emerging Regions (ICTer)*, Colombo, Sri Lanka, pp. 80-83, 2013, DOI: 10.1109/ICTer.2013.6761159.

[11] Shyong Jian Shyu, Efficient visual secret sharing scheme for color images, *Pattern Recognition,* Vol. 39, No. 5), 2006, pp. 866-880.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

- Marek R. Ogiela: Conceptualization. formal analysis, investigation, and supervision.
- Urszula Ogiela: Data curation, methodology, validation, writing - original draft.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

This work has been supported by the funds of the Polish Ministry of Education and Science assigned to AGH University of Krakow. Research project supported by program „Excellence initiative – research university" for the AGH University of Krakow.

Conflict of Interest

The authors have no conflicts of interest to declare.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)