Hybrid Intelligence in Data Privacy Solutions

Marek R. Ogiela
AGH University of Science and Technology
30 Mickiewicza Ave, 30-059 Kraków, Poland
e-mail: mogiela@agh.edu.pl

Lidia Ogiela
AGH University of Science and Technology
30 Mickiewicza Ave, 30-059 Kraków, Poland
e-mail: logiela@agh.edu.pl

***Abstract*—In this paper, we will present the idea of applying the hybrid intelligence technologies in data privacy. This new paradigm joins artificial intelligence (AI) with human intelligence, and allows to support creation of user-oriented cryptographic procedures. Such protocols will apply selected users' preferences in protocols dedicated for increasing data privacy.**

Keywords-Hybrid Intelligence; data privacy; cryptograpic protocols.

I. INTRODUCTION

Modern cryptographic algorithms may be oriented on particular person or group of users. To achieve such feature, it can be implemented using selected AI techniques. There are many contributions presenting security approaches focused on particular users e.g., defining personalized cryptographic protocols [1][2], which can implement personal features or special AI techniques to select unique parameters. Among such techniques we can also find solutions, in which artificial intelligence allows to extract behavioral features or cognitive skills [3][4]. Application of AI procedures allows to define a new area of IT security called cognitive cryptography [5].

Nowadays we can also observe development of new hybrid, i.e., human-AI solutions in security technologies. This means that also in IT security will be possible to introduce hybrid human-AI approaches, which can be focused to guarantee the high security level, and oriented for selected users. Such solutions allow to extend traditional security procedures towards more extensive and optimized analysis of security parameters (or features), and creation of security procedures strongly connected with particular persons. Extensive semantic analysis can be supported by AI solutions, which allow to select the optimal personal parameters or features for created user-oriented security protocols.

Below will be described areas of application of such hybrid procedures, which can be defined for security purposes.

II. HYBRID APPROACHES IN SECURITY PROTOCOLS

The most important areas of application of hybrid security protocols are the following:

- Secure information sharing with privileges
- Knowledge-based authentication protocols
- Visual cryptography
- Personalized behavioral security procedures

In such areas we can define user-oriented security procedures, which involve AI procedures. AI techniques perform optimization tasks, especially important in selection of parameters, or during evaluation of features implemented in security protocols. For example, when we try to define a personalized security protocol we often apply personal features or characteristics. Considering different biometric patterns as well as other specific users features we can evaluate for a particular person a very large feature vector with many personal characteristics. Having such personal record, we can easily select a some of the most distinctive personal features which can later be involved in personalized or user-oriented protocol.

Considering the above mentioned areas of application, we can define the most important features of such protocols as follows.

In secure information sharing, hybrid intelligence can be applied in such manner that user preferences or personal features will have influence on selection of the sharing algorithm, and starting parameters like number of parts, privileges etc. The way of parts distribution can be dependent on AI procedures, which allow to perform division of secret information over several layers.

Knowledge-based authentication protocols can be oriented for particular user or group of persons [6]. In such techniques, expertise knowledge and experiences can be considered, and authentication protocol will be related with thematic visual patterns. Personal features may be related to expertise areas connected with particular user. Having selected the thematic areas AI approaches allow to efficiently select or find visual patterns, which can be presented to user during security procedures.

Visual cryptography is one of the most important areas of application of hybrid intelligence security protocols. Such techniques allow to split visual secret information into several different parts. Usually personal recognition abilities are connected with perception function, and decide when particular user is able to recognize original secret. With such techniques will be possible to establish personal perception thresholds evaluated for different users. Perception levels can

 ISBN: 978-1-61208-969-0

also be dependent on user's knowledge and experiences. In such protocols, knowledge and expectations define human factors, but perception abilities can be evaluated by AI procedures.

Personalized behavioral security procedures allow to define a special type of security protocols, in which different movement feature can be considered [7]. It may contain very simple procedures for personal key generation or more complex protocols oriented for creation behavioral locks. Here we can consider different types of human body movements starting from palm gestures to more complex human motion patterns registered while doing special exercises [1].

In all described areas, the methodology of using hybrid intelligence is the same. To create hybrid human-AI security protocol, firstly the set of personal parameters should be defined. Having defined personal features, the selection of appropriate and unique features can be performed with application of AI methods. The selection of optimal features is usually a very complex task especially in situation when a very large feature vector is available. In such cases, AI approaches allow to quickly select the optimal feature set. Important advantage of application of AI techniques is possibilities to consider constantly changing parameters, which can have different values over the time.

III. CONCLUSIONS

In this paper, we presented possible areas of application of hybrid intelligence techniques used in security protocols. More specifically, the way of application of personal features in advance security solution were described. Additionally, selection of the most important personal parameters can be performed with application of AI procedures.

The most important features of hybrid intelligence security methods are efficiency, and personalization towards application by particular person. Such techniques allow to consider different personal features, and changing parameters associated with users. Hybrid intelligence methods will enrich the cognitive cryptographic approaches defined to join security methods with semantic features or personal parameters [8][9].

ACKNOWLEDGMENT

This work has been supported by the National Science Centre, Poland, under project number DEC-2016/23/B/HS4/00616. This work has been supported by the AGH University of Science and Technology research Grant No 16.16.120.773.

REFERENCES

[1] L. Ogiela, and M. R. Ogiela, "Cognitive security paradigm for cloud computing applications," Concurr. Comput.: Pract. Exp. 32(8), e5316, 2020, doi: 10.1002/cpe.5316.

[2] S. Zapechnikov, "Privacy-Preserving Machine Learning as a Tool for Secure Personalized Information Services," Procedia Computer Science, Vol. 169, 2020, pp. 393-399, doi: 10.1016/j.procs.2020.02.235.

[3] L. Ogiela, "Transformative computing in advanced data analysis processes in the cloud," Inf. Process. Manage. 57(5), 102260, 2020.

[4] M. R. Ogiela, L. Ogiela, and U. Ogiela, "Biometric methods for advanced strategic data sharing protocols,". In: 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing IMIS 2015, pp. 179–183, 2015, doi: 10.1109/IMIS.2015.29.

[5] M. R. Ogiela, and U. Ogiela, "Secure information splitting using grammar schemes," New Challenges in Computational Collective Intelligence. Studies in Computational Intelligence, vol. 244, pp. 327–336. Springer, Heidelberg, 2009, doi: 10.1007/978-3-642-03958-4_28.

[6] C. Guan, J. Mou, and Z. Jiang, "Artificial intelligence innovation in education: a twenty-year data-driven historical analysis," Int. J. Innov. Stud. 4(4), 134–147, 2020.

[7] N. Ferguson, and B. Schneier, "Practical Cryptography," Wiley, 2003.

[8] S. J. H. Yang, H. Ogata, T. Matsui, and N.-S. Chen, "Human-centered artificial intelligence in education: seeing the invisible through the visible," Comput. Educ.: Artif. Intell. 2, 100008, 2021.

[9] M. Del Giudice, V. Scuotto, B. Orlando, and M. Mustilli, "Toward the human – Centered approach. A revised model of individual acceptance of AI," Human Resource Management Review, 2021, 100856, doi: 10.1016/j.hrmr.2021.100856.

 ISBN: 978-1-61208-969-0