Predictive Intelligence Approaches for Security Technologies

Urszula Ogiela[1] and Marek R. Ogiela[2(✉)]

[1] Pedagogical University of Krakow, Podchorążych 2 St., 30-084 Kraków, Poland
[2] Cryptography and Cognitive Informatics Laboratory, AGH University of Science and Technology, 30 Mickiewicza Ave, 30-059 Kraków, Poland
mogiela@agh.edu.pl

Abstract. AI techniques are increasingly being used in security systems. Among them, Predictive Intelligence based approaches can also be used to define new types of security features and cryptographic protocols using perceptual or user-oriented features of authorized persons. This work will describe such the possibilities of using Predictive Intelligence technology in the development of modern data security protocols.

Keywords: Personalized cryptography · User-oriented security systems · Eye tracking technologies

1 Introduction

Predictive Intelligence is a new approach based on intelligent data analysis, which is especially connected with consumers, and which evaluate users' profile and characteristics with the purpose of forecasting their future actions or behaviors. Predictive Intelligence very often relies on user interaction with services and query data, what allow to predict future trends and behaviors. Such techniques are often applied in social sciences, as well as business and management applications. Despite it is closely related to AI applications, it can also be applicable in many engineering technologies and advanced information processing systems. Predictive approaches can considerably enhance computing possibilities and increase the efficiency of information acquisition, analysis, and exploration, using especially computational intelligence approaches, collective and cognitive computing. It can also be applied for knowledge engineering and information management tasks, especially thanks to developing new prognostic or cognitive-based inference approaches [1, 2].

Such techniques additionally open new possibilities for efficient and secure data processing in security systems, especially when dealing with a great amount of data in social apps, Cloud, and multimedia systems. In next sections will be described possible applications of such technologies in creation of security procedures for transformative computing and human centered security solutions [3, 4].

L. Barolli (Ed.): BWCCA 2021, LNNS 346, pp. 193–196, 2022.
https://doi.org/10.1007/978-3-030-90072-4_20

2 Security of Human-Oriented Systems

Predictive Intelligence uses personal behavioral patterns to determine future user actions or preferences. Such characteristics can also be used in the development of new security protocols oriented towards individual participants of such protocols. Predictive analysis can involve the application of not only consumer preferences or behavioral patterns, but also personal characteristics in the form of biometrics or perceptual features. Actually, exist many security protocols that use cognitive techniques and biometric features of users [5, 6]. In such systems, therefore, there arises the possibility of applying predictive intelligence techniques to extract the behavioral patterns of individual users and then using them to define personalized cryptographic solutions that would be dedicated to particular users and consider only their personal characteristics or individual behavioral patterns. Having such solutions, it is possible to create a number of cryptographic procedures which increase the level of data security, or personalized user authentication. Possible applications include such important solutions as generation of personalized encryption keys, protocols for dividing secret information based on individual characteristics, or steganography of multiple secrets [7].

Predictive Intelligence is strongly related not only to users' preferences, but also to their perceptual characteristics and cognitive abilities. All user preferences are originating from associative and cognitive properties. This means that predictive intelligence can also be used in the so-called, cognitive cryptography defined in [1]. Cognitive cryptography systems are based on the use of cognitive information systems, which allow the extraction of individual personal characteristics or perceptual thresholds. Predictive intelligence techniques can also be used for such analysis, which cannot only facilitate to determine current user preferences and behaviors, but also predict how they will evolve and change, when the user acquires knowledge and experiences [8].

3 Predictive Analysis in Transformative Computing Systems

Another important application of predictive intelligence is transformative computing technologies. This technology uses AI algorithms to analyze the collected data, acquired by sensor networks. This allows the implementation of IoT systems, as well as the creation of systems that work adaptively depending on the external environment, in which they operate, or in which the user is located. Changes in the external environment are constantly monitored by sensor networks and allow to make the functioning of programs or services dependent on a specific environment. A similar situation can occur with relation to individual users, where protocols or services can only function if they are run by authorized users, or people who are in the right place or environment. In this technology, an important issue is the security of collected and processed data, as well as the possibility of fast authorization of users, in order to confirm their rights to use particular protocols. To this end, interesting solutions based on cognitive systems have been proposed and described in [3].

One of the possibilities of their extension is also the use of predictive intelligence techniques to analyze the changing environment in which the user legitimately uses selected computer services. This is important when the external environment is constantly changing and the availability of a given service depends on external factors. In

this case, predictive intelligence allows to estimate the directions of changes of external parameters and to confirm whether the user will still be able to use a given service after their change. Changes in external factors must be monitored by sensor systems related to the user or the surrounding environment. This is how predictive algorithms can help extend the functionality of transformative computing technology [9].

As mentioned before transformative computing technologies use intelligent AI algorithms to analyze clustered data or sensory signals. Such analysis is aimed at finding solutions to analytical or semantic problems. As shown in the paper [1], instead of classical AI solutions, one can also use cognitive information systems that allow to apply procedures oriented on extraction the meaning of data and understanding information. It is in this approach that predictive intelligence techniques can additionally be used to further identify possible changes or predict the directions of user behavior and their use of services and services [10].

4 Conclusions

This work describes possible ways of using predictive intelligence technology in cryptography and security areas. This technology used so far in forecasting and prediction may also be used in creating security procedures associated with individual users. Such procedures may use individual characteristics of particular persons, but also their application may depend on external conditions and user privileges. In such a situation, predictive intelligence mechanisms allow to make predictions about changes in external conditions, and allow to monitor users' permissions to use given resources or services. As shown in this work, predictive intelligence techniques can replace traditional AI methods used in security procedures, but also increase the functionality of semantic analysis performed by cognitive information systems, which takes place in transformative computing. This allow to extend the application areas of such technologies towards intelligent security protocols, which are oriented for particular user, and not only evaluate and apply his/her personal patterns or characteristics, but also allow to predict users' behaviors, and forecast changes in external environment. On the other side in predictive analysis it will be possible to use cognitive reasoning approaches imitating the way of human thinking, and implementing resonance processes in the same way as these existing in human mind.

Acknowledgments. This work has been supported by Pedagogical University of Krakow research Grant No BN.711-79/PBU/2021. This work has been supported by the AGH University of Science and Technology research Grant No. 16.16.120.773.

References

1. Ogiela, L., Ogiela, M.R.: Cognitive security paradigm for cloud computing applications. Concurr. Comput.: Pract. Exp. **32**(8), e5316 (2020). https://doi.org/10.1002/cpe.5316
2. Ancheta, R.A., Reyes, F.C., Jr., Caliwag, J.A., Castillo, R.E.: FEDSecurity: implementation of computer vision thru face and eye detection. Int. J. Mach. Learn. Comput. **8**, 619–624 (2018)

3. Ogiela, L.: Transformative computing in advanced data analysis processes in the cloud. Inf. Process. Manage. **57**(5), 102260 (2020)
4. Ogiela, M.R., Ogiela, L., Ogiela, U.: 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). https://doi.org/10.1109/IMIS.2015.29
5. Ogiela, U., Ogiela, L.: Linguistic techniques for cryptographic data sharing algorithms. Concurr. Comput.: Pract. Exp. **30**(3), e4275 (2018). https://doi.org/10.1002/cpe.4275
6. Ogiela, M.R., Ogiela, U.: Secure information splitting using grammar schemes. In: Nguyen, N.T., Katarzyniak, R.P., Janiak, A. (eds.) New Challenges in Computational Collective Intelligence. Studies in Computational Intelligence, vol. 244, pp. 327–336. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03958-4_28
7. Ogiela, L., Ogiela, M.R., Ogiela, U.: Efficiency of strategic data sharing and management protocols. In: The 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-2016), 6–8 July 2016, Fukuoka, Japan, pp. 198–201 (2016). https://doi.org/10.1109/IMIS.2016.119
8. Guan, C., Mou, J., Jiang, Z.: Artificial intelligence innovation in education: a twenty-year data-driven historical analysis. Int. J. Innov. Stud. **4**(4), 134–147 (2020)
9. Menezes, A., van Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography. CRC Press, Waterloo (2001)
10. Yang, S.J.H., Ogata, H., Matsui, T., Chen, N.-S.: Human-centered artificial intelligence in education: seeing the invisible through the visible. Comput. Educ.: Artif. Intell. **2**, 100008 (2021)