Semantic Approaches for Cognitive Data Processing

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

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

Abstract— **This paper describes a semantic-based technique for intelligent data processing and cognitive analysis. The described methods are used to create knowledge extraction procedures, which apply the semantic content and meaning for data handling. Such methods are designed for efficient data management and protection in cloud environment.**

Keywords-Cognitive reasoning; data processing and management; semantic description.

I. INTRODUCTION

Modern security protocols very often use semantic content description of secured data and involve it in creation of security algorithms. Such methods were proposed in the new area of cognitive cryptography in [1][2]. In such methods the semantic content should be evaluated and applied in the security protocol, which finally results in the encrypted data being dependent on its semantic meaning. Such protocols define an important extension of traditional security procedures, which usually do not make any connection between semantic content and final encryption results.

Similar connections to the ones mentioned in the previous paragraph between semantic content and protocols can be implemented in data management techniques as well. Such techniques will be described in following sections, in which we will define semantic-based secure data management approaches. The main idea of such procedures is to create a new class of strategic data management procedures oriented for information splitting and distribution in complex, hierarchical management structures. Information splitting and distribution will be strongly dependent on the content of shared data [3]-[5]. The main action of such techniques will be connected with a semantic content evaluation, which will provide the data feature vector. Feature parameters from this vector will be used in the information division task.

The rest of the paper is structured as follows. In Section II, we present the concept of data management using semantic information. In Section III, we mention some applications of management protocols. We conclude the paper in Section IV.

II. DATA MANAGEMENT USING SEMANTIC INFORMATION

In order to define semantic-based management algorithms, it is necessary to introduce two different types of protocols. The first type of protocols includes techniques which allow to evaluate the semantic content of encrypted information. The second type of protocols contains efficient data division protocols which allow to share secret data into a particular number of parts, which can then be distributed among users in management procedures. In such techniques, the distribution of secret parts should be connected with the content and implemented with the application of semantic parameters extracted at the beginning of the procedures.

For extraction of semantic description, we can use the cognitive information systems defined in [1][6]. In the past, several different classes of cognitive procedures were defined, which focused on the evaluation of different types of data, from visual patterns, to economical or secret data.

Cognitive systems are aimed at extracting the semantic content from analyzed data and evaluating some important knowledge which is present in the data. Very often, this requires extensive analysis, including the application of advanced Artificial Intelligence (AI), or cognitive resonance procedures. As a result of cognitive analysis, it is possible to build a data record which contains the semantic description of the analyzed information. Such semantic record can contain a large number of parameters describing different global or local features. Depending on the goal of the information splitting in management procedures, it is possible to select the most important parameters from this information, which can then be applied to perform the data splitting and distribution tasks in an efficient and secure manner.

When we select several semantic features, we can implement them using a division and management protocol. To perform such task, first, it is necessary to select a data sharing technique [3][5] and apply it for complex hierarchical management structures. To do this, it is necessary to determine the number of levels and layers in the hierarchical structure, as well as the number of participants at each level. Having selected the parameters and having evaluated the semantic features of the divided information, we can start the division procedures with the following input parameters:

- semantic factors,
- defined numbers of layers and participants,
- secret information that needs to be splitted,
- starting parameters for sharing procedures.

After finishing secret data division sequences, we obtain a particular number of secret parts, which can then be distributed to each level in the hierarchical structure. Distribution can be done in different ways depending on the number of persons and the access privileges. We can consider a specially defined distribution topology for the obtained

 ISBN: 978-1-61208-972-0

secret parts, which can be placed in an irregular manner over different levels in the hierarchical structure.

III. Application of Management Protocols

The defined semantic-based sharing and management procedures have several possible areas of application. Such techniques extend classical management procedures towards including semantic content. Such techniques are dependent on features, and the information can be splitted and distributed in different ways. The possibilities of selection of semantic parameters introduce an additional security level because the whole protocol allows to reconstruct the original data only in the situation when the input parameters are known. The knowledge about the procedure will not be enough to perform unauthorized data reconstruction from the generated parts.

The security feature allows to apply these types of protocols in different management or security areas. In particular, they may be applied in secure and trusted data management in distributed systems, like cloud structures [7][8]. It can be also implemented in distant services management, as well as secure data storage and distribution. Performing analytics tasks with the application of semantic feature on the analyzed data makes such protocols also applicable in predictive analysis towards prognosis of user trends or behaviors [9][10].

IV. Conclusions

In this paper, we described a new idea of creation and application of semantic-based protocols in security areas. Such methods can be used in a broad range of management activities, especially connected with secret data division in complex and distributed structures. The main idea of such protocols lays in the extraction of the semantic meaning of encrypted data and the application of such information in security protocols. The extraction of semantic meaning can be done with the application of cognitive information systems, and the extracted features can decide about the way of information encoding and distribution. Such techniques can be widely applied in cloud computing and distributed services management, as well as secure data distribution in complex structures. Such methods enrich traditional management approaches and have influence in the creation of new security protocols in cognitive cryptography [1][11].

Acknowledgment

This work has been supported by the National Science Centre, Poland, under project number DEC-2016/23/B/HS4/00616.

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] 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.

[3] 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.

[4] S. Nakamura, L. Ogiela, T. Enokido, and M. Takizawa, “Flexible Synchronization Protocol to Prevent Illegal Information Flow in Peer-to-Peer Publish/Subscribe Systems,” in: Barolli, L., Terzo, O. (Eds.), Complex, Intelligent, and Software Intensive Systems, Advances in Intelligent Systems and Computing. 611, pp. 82-93, 2018.

[5] N. Ferguson and B. Schneier, “Practical Cryptography,” Wiley, 2003.

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

[7] R. A. Ancheta, F. C. Reyes, J. A. Caliwag, and R. E. Castillo, “FEDSecurity: implementation of computer vision thru face and eye detection,” Int. J. Mach. Learn. Comput., 8, pp. 619–624, 2018.

[8] S. Gil et al., “Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges,” Internet of Things, 8, 100118, 2019.

[9] 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.

[10] 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.

[11] 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: 978-1-61208-972-0