Transformative Computing for Cyber-Security Protocols

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

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

***Abstract*—This paper will discuss the main techniques based on transformative solutions, dedicated to data protection and security. Transformative computing is designed to collect and analyze data obtained from various sources, taking into account their updates and changes. The analysis of data obtained from various sources is possible by using linguistic and semantic techniques to describe and interpret data in order to properly extract information contained in large data sets. Linguistic techniques guarantee the proper description of the analyzed data and the selection of relevant information in a given analysis process. These processes allow for proper data protection both in common use systems and in cyberspace.**

Keywords-Transformative computing; linguistic techniques; cyber-security protocols.

I. INTRODUCTION

Transformative computing methodology is dedicated to the implementation of complex and large data sets processing, obtained from various sources, at various times, recorded by various recorders [2][4][5]. Thus, these are calculations that process different data sets. Their diversity allows to obtain information of great importance for the data processing process. Determining the meaning is possible thanks to the use of linguistic techniques in the process of interpretation and inference. Linguistic techniques dedicated to the tasks of meaningful interpretation of data allow to obtain information that can significantly affect the process of automatic data understanding [6][7]. Data understanding processes, on the other hand, are an innovative solution in the field of constructing data protection and security protocols. The main area of application of the discussed solutions are cryptographic threshold schemes, intended for data security tasks through their sharing [1][3][7].

The novelty presented in this paper is the possibility of dedicating transformative techniques to the processes of data security for cyber-security protocols.

The rest of the paper is structured as follows. In Section II, we introduce the concept of the Transformative Computing paradigm. In Section III, a security protocol based on linguistic threshold schemes will be described. Finally, we conclude the work in Section IV.

II. TRANSFORMATIVE COMPUTING METHODOLOGY

Transformative computing methodology is used to implement complex computational processes. Their important aspect is that the data on the basis of which the calculations are made, may come from various sources recording information in real time. An important advantage of such computing is therefore the ability to combine data sets of different nature, size and format. This is possible thanks to the use of techniques that are primarily used to extract important (from the analysis point of view) information that is important for the process of description and inference. This stage is carried out on the basis of the use of linguistic techniques in the process of describing the interpreted data.

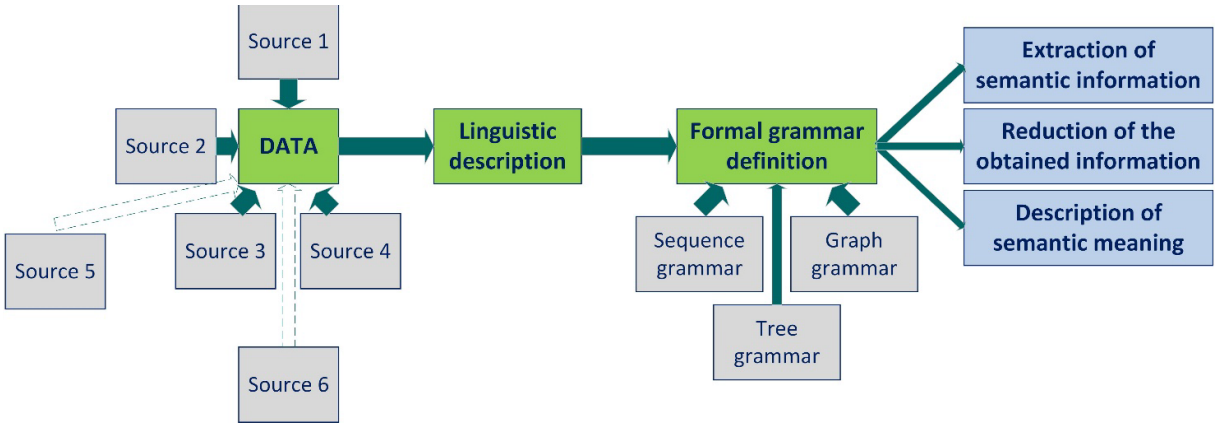

Figure 1. Transformative computing methodology.

Copyright (c) IARIA, 2023. ISBN: 978-1-68558-037-7

Linguistic techniques allow the extraction of semantic information contained in data sets. This information is used to describe the importance of the analyzed collections and thus allows for a significant reduction of the obtained information. At this stage, the method of description the analyzed data is also selected, using linguistic techniques of data interpretation in the form of formal grammars. The choice of the right grammar rules depends on the type of data for which the analysis is carried out, but it is focused on the choice of sequence, tree or graph grammar. A schematic representation of the transformation calculation process is shown in Figure 1.

III. CYBER-SECURITY PROTOCOLS

Data security protocols based on the use of linguistic techniques for the proper extraction of data constituting secret information that may be subject to confidentiality processes are gaining more and more importance. Their main task is to protect and secure confidential, secret or strategic data. High-priority data protection are in classical cryptographic systems, but also in the cyber security. The idea behind the new generation of solutions is the ability to use effective methods of securing data with a high security priority. A new solution is the possibility of using linguistic techniques in threshold schemes to provide a semantic description of a shared secret and the possibility of splitting data obtained from transformative computing. An important advantage of this solution is the acquisition of relevant data with semantic meaning while eliminating irrelevant or low-importance data. In addition, this solution allows the use of linguistic techniques in the process of dividing a secret between a specific group of secret keepers. At the same time, the semantic analysis of the secret may constitute its part as an element subject to secrecy. The method of choosing the optimal data protection protocol takes place at the stage of defining the threshold scheme that is to be used to implement the data protection process (Figure 2).

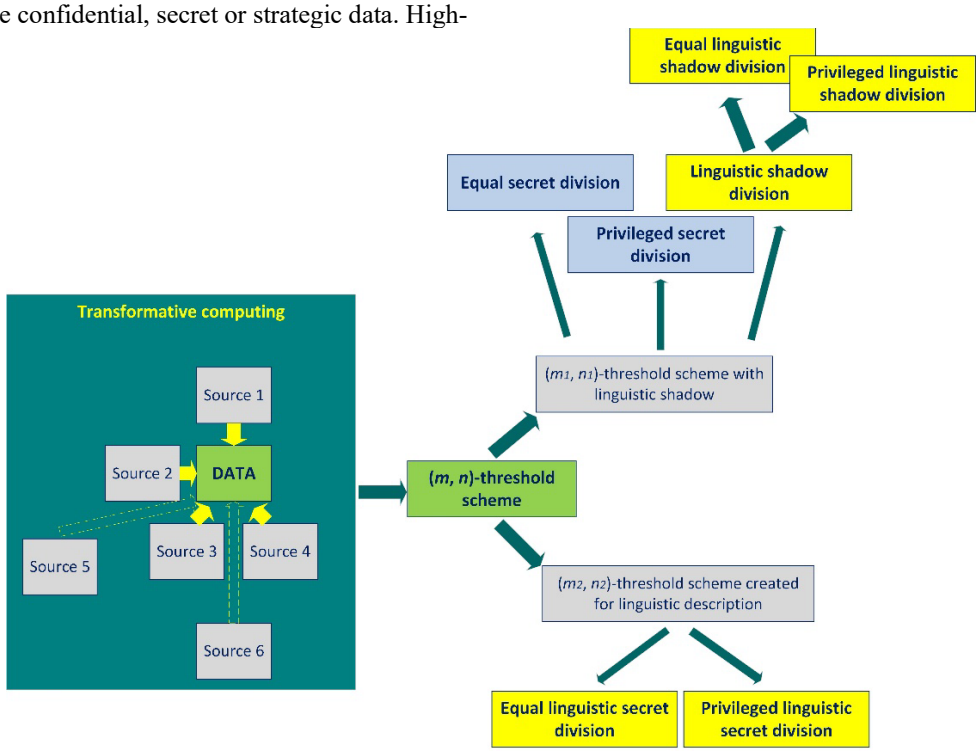

Figure 2. Transformative computing for linguistic threshold schemes in security protocols.

Linguistic techniques included in the data protection process based on threshold schemes, can be used in data protection processes in cyber security. Their advantage is high flexibility resulting from the possibility of selecting data recording sources for the implementation of transformative computing, the use of universal secret description techniques using linguistic methods, and the use of linguistic threshold schemes that guarantee an accurate description of the secured data enriched with elements of semantic description.

Data security protocols dedicated to cyber security guarantee high security and the possibility of their continuous modification due to emerging changes in procedures, opportunities and threats, both external and internal. The threshold schemes proposed in this paper, based on transformative computing methodology and semantic inference techniques, guarantee a high level of data protection. Transformative computing combined with linguistic reasoning techniques can be applied to multi-level structures, which makes it much easier to manage them from different levels of the entire process and structure. Such a solution can therefore be effectively used in cyber security, where data security processes are carried out at various levels. The universality of the presented solution results from the use of transformative computing techniques in the process of obtaining and processing data, which constitute information of a secret nature, results from the possibility of extracting the

Copyright (c) IARIA, 2023. ISBN: 978-1-68558-037-7

semantic meaning only for relevant data, and from the possibility of constructing threshold schemes in order to divide the secret along with its semantic description (contained in the additional secret shadow) between the secret trustees.

IV. CONCLUSIONS

This paper presents an innovative approach to the process of securing data using linguistic threshold schemes, in which semantic information presenting the meaning of the secret plays an important role. The linguistic description of the secret is the result of data processing based on transformation techniques that allow the collection and processing of various data sets from different data recorders. The universality of the discussed solutions allows for their wide application, especially in cyber security.

ACKNOWLEDGMENT

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

REFERENCES

[1] M. Biro, A. Mashkoor, and J. Sametinger, "Safety and security of cyber-physical systems," J. of Softw.-Evol. and Proc. e2522, 2022, doi: 10.1002/smr.2522.

[2] S. Gil at al., "Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges," Inter. of Things. Vol.8, paper 100118, 2019.

[3] A. Menezes, P. van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography." CRC Press, Waterloo, 2001.

[4] Y. Moustafa and F. Kawsar, "Transformative computing and communication," Computer. Vol. 52 (7), pp. 12-14, 2019.

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

[6] 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.

[7] M. R. Ogiela and L. Ogiela, "Cognitive cryptography techniques for intelligent information management," Int. J. of Inf. Manage. 40, pp. 21-27, 2018, doi: 10.1016/j.ijinfomgt.2018.01.011.

Copyright (c) IARIA, 2023. ISBN: 978-1-68558-037-7