Proceedings of the 33rd International Conference on Information Technologies (InfoTech-2019)
19-20 September 2019, Bulgaria

CYBER SPACE FEATURES – SECURITY AND DATA PROTECTION REQUIREMENTS

***Digest of paper*[1]**

Radi Romansky, Irina Noninska

Technical University of Sofia
e-mails: rrom@tu-sofia.bg, irno@tu-sofia.bg
Bulgaria

Abstract: The paper deals with users' security and protection of personal data in the digital space. A short presentation of the features of contemporary cyber technologies related to the user's privacy is made. A summarization of the main challenges is presented and some requirements for privacy protection are formulated.
Key words: digital age; cyber technologies; privacy; data protection, user's security.

1. INTRODUCTION

Information Society (IS) is based on the contemporary Information and Communication Technologies (ICT) used in different spheres of public and social life. The importance "to be innovative and competitive in today's global digital economy" is discussed in [1]. The digital activities could disturb the individual privacy of these persons which take part in the network communications and requests strong control and protection of personal data [2]. In this reason the European General Data Protection Regulation (GDPR) [3] determines a basic frame for keeping user's privacy and strong regulation [4, 5]. Personally, article [5] discus genetic data processing and the necessity of strong protected because they consist of sensitive. The digital age is based on the new technologies, as cloud computing (CC) & mobile cloud computing (MCC) [6], Internet of Tings (IoT) [7], and Big Data & Big Data Analysis [8, 9] and the article summarizes basic requirements for keeping user's privacy and data protection.

2. DIGITAL SPACE – HISTORY AND FEATURES

A brief summary of the historical aspects of the expression "information society" is presented, started by the first proposal in written text by the author Jiro

[1] The full paper is proposed for including in the IEEE Xplore Digital Library

Kamishima and the editor Michiko Igarashi (January 1964) [10]. Different definitions have been proposed in the next two decades and finally the shortest definition for the IS has been adopted: "*The transition of the industrial society to the new information society is realized if over 50% of the people are employed in the sphere of information-intellectual services*".

The basic features of the IS could be determined as follows: *Essence* (information and knowledge are the major products); *Objective*; *Virtualization*; *Integration*; *Humanization*; *Globalization*; *Dynamics*; *Innovation*. Based these features the goal of the IS is to create suitable and efficient information environment and systems for providing modern management and remote access to information resources in different nodes of the network space by combining different components. The solution of this global is related to the following two key elements: *Information resources* & *Information security*.

3. CYBER TECHNOLOGIES AND PRIVACY

The IS-features extend the role of the contemporary technologies in the personal life and business processes but they have challenges for privacy of the humans [11].

Social computing (SoC) is an interactive communication between persons by using environments united as a Social Networking Sites (SNS), but can create a risk for privacy and personal data, because the information is disseminated to many other users, including unknown persons [12].

Cloud computing relates to the cross-border data transfers, including personal data and this could violate the GDPR requirements concerning their protection. In this reason special measures for data protection in cloud should be taken into account [13].

Internet of Things (IoT) unites rules, protocols, standards and applications for managing the connection with devices and sensors ensuring distance control of monitored parameters. The article [7] discusses the relation between processes success and the characteristics of the IoT. On the other hand, IoT marks a tendency of the growing usability and its role in the everyday life of people increases. This outlines significance of the procedures for user's privacy protection and necessity of providing reliable information security.

Big Data Analysis (BDA) permits to process and analyse collected large sets of data for any purpose [8] which can be very important for research in spheres as industrial, health, education, etc., but this analysis could be "more complex and difficult to manage" and the persons' privacy could be disturbed [9].

4. CHALLENGES FOR SECURITY AND PRIVACY

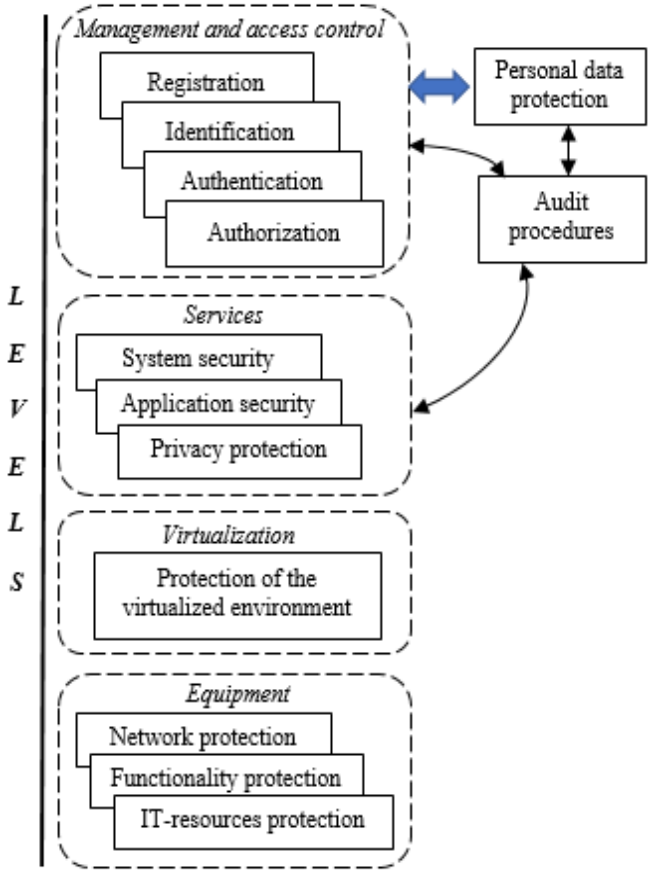
The cyber space is based on remote access to resources in information environments (IE) which must organize the information service, including registration module and collection of users' personal data (PD) in own database. The registration requests provision of certain categories PD that are stored (and processed) by the IE-owner. The following questions arise: ✓ How and where are stored these personal data? Who can access them, and what regulations are valid for them? ✓ Who should

protect user's PD and who must make the solutions from change and destruction of data? ✓ What policies must be applied for storing personal data and keep confidentiality during their processing via digital spaces? ✓ How could guarantee personal data integrity and their correct transfer between different nodes of the global network. Answers to these and other questions will be addressed in the following themes: ✓ Do social networks protect personal data? ✓ What happens with the personal data in the Cloud? ✓ Are there any problems with the privacy at the IoT? ✓ Does privacy is protected in Big Data Analysis? ✓ How to determine who is a "Data Controller" and which one is the right law enforcement mechanism?

5. SECURITY AND DATA PROTECTION REQUIREMENTS

In order to overcome these possible problems for the user's privacy, effective implementation of legal and technical requirements and full interaction between citizens, business and administration are of a great importance. All these requirements must be directed to keeping the privacy. An example is the cloud which proposes a common virtual space for many customers (multitenancy) and summarization of the possible security problems is made in table 1.

The main security treats in the cloud environments relate to the multi-tenancy because many users could access the stored data by mobile devices and share single software or application. This create a risk for the confidentiality and requires strong control including personal identification and authorization. The security activities must be done on each level and for this purpose an organization of a System for Information Security (SIS) is presented in the next figure.



Security organization to protect resources in cloud services

It is important to emphasize that the IoT security is not only devices' and network security. All components should be considered, including network interfaces, software, mobile apps, USB ports, cloud, etc. In this reason some important requirements relevant to IoT could be determined, as follows:

✓ Connectivity between things must be realized after their identification.

✓ Interoperability must be ensured among different systems which are in communication.

✓ Autonomic networking and servicing must be provided to support precise network functionality and automatic processing the data of things.

✓ Security for the IoT is an important requirement because every "thing" deals with data which can be treated for confidentiality, authenticity and integrity of data including personal data too.

✓ Privacy protection should be taken into account in IoT since many things are related to everyday life, as a result humans' different sensitive data are collected and processed. This requirement must be supported during all stages of activity as data collection and transmission, aggregation, storage, mining, processing, analysing, etc.

Table 1. Summarization of Possible Problems in the Cloud

Security type	***Main problems***
Communication security issues	Free sharing of the infrastructure
	Different virtual networks using
	Misconfiguration of communication
Architectural security issues	Arbitrary resource virtualization
	Improper data and storages organization
	Unprotected web applications using
	Weak access control
	Bad digital right management
Contract aspect	Unsecure servicing and dissemination
	Illegal personal data dissemination

Similar issues can also be asked for the social computing and the main recommendation that must be extremely accurate dealing with the required information. Users must have good opportunity to be informed in time about any case of privacy violation. Everyone should have knowledge about what kind of personal data will be processed.

6. CONCLUSION

The mine requirements for the information security in the cyber space can be summarized as a protection of the integrity (from unauthorized deletion, modification, theft) and the availability (access to services, data and resources anywhere and anytime). The requirements for data protection are determined in the document GDPR with paradigms "right to be forgotten" (erasing all personal data after finishing the goal of processing) and "privacy by default", which means that the default settings should ensure maximum privacy.

ACKNOWLEDGMENT

The research is conducted under the grant of project DH07/10-2016, funded by Bulgarian National Science Fund, Ministry of Education and Science.

REFERENCES

[1] W. Van Grembergen, and St. De Haes, "Introduction to the minitrack on IT governance and its mechanisms", *Proc. of the 51st Hawaii International Conference on System Science*, 2018, pp. 4877-4879 (https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1578&context=hicss-51)

[2] J. A. Obar and A. Oeldorf-Hirsch, "The biggest lie of the Internet: ignoring the privacy policies and terms of service policies of social networking services", *Journal Information, Communication and Society*, July 2018 (https://www.tandfonline.com/doi/abs/10.1080/1369118X.2018.1486870)

[3] W. R.M. Long, G. Scali, Fr. Blythe, and A. Ch. Raul, "European Union overview", chapter 2 in the book "*The privacy, data protection and cybersecurity law review*" (5th ed.), Law Business Research Ltd, October 2018, pp.5-39.

[4] W. G. Voss. "European Union data privacy law reform: General Data Protection Regulation, privacy shield, and the right to delisting", *Business Lawyer*, 1 (vol. 72), Jan 2017, pp. 221-233.

[5] M. Shabani and P. Borry, "Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation", *European Journal of Human Genetics*, vol. 26, 2018, pp. 149-156.

[6] C. V. Raja, K. Chitra and M. Jonafark, "A Survey on Mobile Cloud Computing", *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 3 (vol. 3), 2018, pp.2096-2100.

[7] M. Ammar, G. Russello and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks", *Journal of Information Security and Applications*, vol. 38, Feb 2018, pp.8-27.

[8] D. Ivanova and A. Elenkov, "Big Data Analytics for air quality monitoring assessment based of IoT platform", *International Journal on Information Technologies and Security*, 2 (vol. 11), 2019, pp.43-50.

[9] D. Zhang, "Big data and privacy protection", *Proc. of the 8th International Conference on Management and Computer Science*, October 2018, Advances in Computer Science Research, vol. 77, Atlantis Press, pp.275-278.

[10] L. Z. Karvalics. "*Information Society – what is it exactly? (The meaning, history and conceptual framework of an expression)*". Budapest, March-May, 2007, 26 p.

[11] R. Romansky, "A survey of digital world opportunities and challenges for user privacy", *International Journal on Information Technologies and Security*, ISSN 1313-8251, vol. 9, No. 4, December 2017, pp. 97-112.

[12] R. Romansky, "Social Computing and Digital Privacy", *Communication & Cognition*, ISSN 0378-0880, Belgium, vol. 48, No. 3-4, November 2015, pp.65-82.

[13] J. Shen, T. Zhou, X. Chen, J. Li, W. Susilo, "Anonymous and traceable group data sharing in cloud computing", *IEEE Transactions on Information Forensics and Security*, vol. 13 No. 4, 2018, pp. 912-925.