A SURVEY ON DIGITAL WORLD OPPORTUNITIES AND CHALLENGES FOR USER'S PRIVACY [1]

Radi Romansky

Technical University of Sofia, Department of Informatics
e-mail: rrom@tu-sofia.bg
Bulgaria

Abstract This paper is a summary on the opportunities of the contemporary digital environments and proposed services in the network world and discusses some important challenges for the users' privacy and security. The cyber security and personal data protection are important themes discussed in different levels, including European Commission, US Department of Homeland Security, corporative boards, etc. In this reason, the article presents the main obligations of the administrators, data controllers, data processors, service providers, etc. for protection of the user's personal data and privacy. The discussion is made in the frame of digital world opportunities as e-services, e-governance, e-learning, cloud and social computing, Internet of Things (IoT), Machine to Machine communications (M2M), etc. A summary of the main challenges of digital spaces which could disturb the user's privacy is made and an organizational structure of System for Information Security Management (SISM) is proposed.

Key words: digital age, information servicing, privacy, cyber security, secure access.

1. INTRODUCTION

The main components of the contemporary Information Society are information resources that are distributed in different palaces of the global network. On the other hand, it exists the concept that the Information Society is based on the information as a knowledge that create new knowledge. Different publications determine the term "information resources" as an important element of network infrastructure that contains significant and relevant data used directly by the users. The main goal of the Information Society is to increase the economic, social and cultural levels by using Information and Communication Technologies (ICT).

Many research projects and publications discus and investigate the special features of the digital environments and proposed services in the areas of e-society (e-government [1, 2], e-learning [3, 4], e-business, e-health, etc.), cloud [5, 6] and social [7, 8] computing, smart city (Internet of Tings [9], Machin to Machin communications [10], etc.). The opportunities

[1] This paper is a renewed version of the article presented at the 31st International Conference on Information Technologies (InfoTech-2017), 20-21 September 2017, Bulgaria (http://infotech-bg.com)

of these technologies are significant but it is needed to know that they could create problem for user's privacy based on illegal and/or unauthorised using and transfer of personal data uploaded in user's profiles. For example, using cloud services and social environments permits storing personal data from the user's profiles in different (unknown for data owner) places in the global network. This fact could create some problems for the user's privacy – individuals or business organizations, in the age of information [11]. For example, a security framework for business cloud is discussed in [12] and a survey of opportunities and challenges of the security in cloud computing is made in [13]. Practically, all processes in the digital world should be analysed on the base of privacy and personal data protection. In this reason, the problems with user protection, security in cyberspace and data protection are in the focus of Council of Europe [14] and European Commission [15].

The purpose of this article is to make a summary of the current opportunities of the contemporary digital environments and proposed services, but on the base of the challenges for user's privacy and security. In this connection, the general aspects of the personal data protection (PDP) are summarized in the next Section 2 and the opportunities of the digital world are discussed in the Section 3. Section 4 deals with main challenges of the network environments which could disturb the user's privacy and an organizational structure of System for Information Security Management (SISM) is proposed.

2. SPECIFIC ASPECTS OF THE PERSONAL DATA PROTECTION

Personal Data Protection (PDP) includes activities that must secure the rights of the individuals if their data are used by "data controllers" and/or "data processors". Each administrative structure processing personal data should develop a System for Information Security and Privacy (SISP) – an organizational scheme of such system has been proposed in [16] and it is shown in fig. 1. The main requirements are determined on the base of Data Protection Policy as a part of IT Policy and Security Policy.

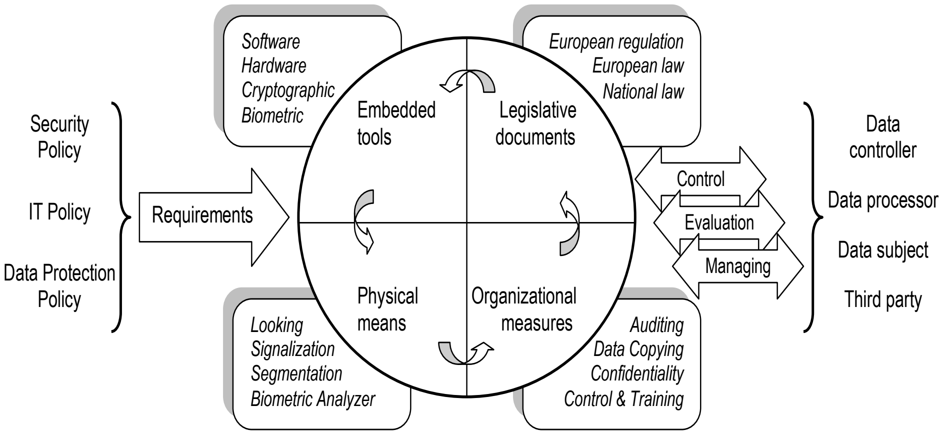


Figure 1. Organizational scheme of SISP [16]

The structure of SISP includes components with hierarchical importance in 4 layers:

(1) Embedded tools is the computer layer and unites software and hardware instruments including cryptographic and biometric means) used in the personal access to the systems

units and resources (for registration, identification, access regulation by authentication, rights for information resources using by authorization, etc.);

(2) Physical (technical) means are realized in the second layer for restriction of unauthorized access by technical blocking, separation of LAN segments, recognition of legitimate users by cameras or cards, etc.

(3) The third layer unites organizational measures as rules, instructions and procedures for administrative control and protecting;

(4) Legislative documents (legislation in national and European levels) are included in the external layer and have limited impact on the real data protection.

This hierarchical sequence should determine the needed and enough level of PDP and to oppose to all ventures to disturb individual's privacy.

The European understanding for "personal data" is the information that permits to identify a person directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity [17]. A popular definition in USA is connected to the rights and obligations of the individuals and institutions about collection, using, keeping and disclosing personal information.

Some important terms listed below are used in the field of PDP.

✓ Processing of personal data – one or more operations with personal data using automatic or non-automatic means;

✓ Data subject – this is the owner of the processed personal data;

✓ Data controller – person or organization who organizes and support data processing based on previously determined goal and must be responsible for all procedures with personal data;

✓ Data processor realizes the real processing of personal data on the base of agreement with the data controller;

✓ Receiver of personal data – third party that could receive and use part of all personal data from a data controller on the base of lawful reason only.

Data controller should collect personal data of data subject based on a legitimate reason only and with the consent of the individual. This activity should be realized based on preliminary defined goal and criteria for organization, creation and actualization of registers for personal data. The access to these register (to the personal data stored in the registers) must be made by legitimate persons only on the base of principles of information security: authentication (by using username, password, digital certificate, personal identification number, and biometric means); authorization (on the base of developed digital right management system); accountability (personalization of the access to the data structures and registration of users' activities). All stored personal data in the registers must be full and actual in the each moment of data processing (integrity and content management). If the goal of personal data processing is realized the personal data must be archived or destroyed. Giving personal data to third party or transfer to other country must be realized on the base of strong rules only.

What is the relation of PDP to the contemporary digital word? The possibilities for free connection between people in the global network and other opportunities as remote access to information resources (including personal profiles), collaboration in communities, using cloud services, etc., impose a new demand for strong protection of personal data and information content. This problem is actual for many environments and services in the digital world – e-governance, e-learning, e-health, cloud computing, social media and networks, smart city, Internet of Things, etc. Three basic groups of privacy and security requirements are determined for deciding the problems of PDP [18]: *user privacy* (identifying the purpose of data collection, knowing privacy policy, data erasing after necessity of using, etc.), *network privacy* (all resources are vulnerable to network attacks) and *security mechanisms* (authentication, creation user's profile, protection of learning materials, certification, biometric identification, identification by smart cards, etc.).

3. THE CONTEMPORARY DIGITAL WORLD

e-Governance components and environments.

The idea for digitalization of processes in governance is not new, but it is in growth continuously. The main goal of e-governance is to approve the principles of the constitutional state at the processes in the society. This government of law includes the right for access to information, privacy and protection of personal data, better relations between citizens and public authorities, effectiveness of state governance, increasing quality of services, etc.

E-governance is an approach for realization of the processes in the society by using contemporary ITC and it requires new strategies and policies for democratic governance. Some of the basic components of the e-governance and the place of the e-government are presented in figure 2 and they determine some features:

- the components of e-governance are realized on the base of remote access to information resources and distributed processing via Internet;
- e-governance must be realized by using all democratic principles in the society;
- the social and economic aspects should be reflected in the structures of e-governance;
- e-government (as a part of e-governance) uses a model for relations between 4 groups of participants (administration, government structures, citizens and business).

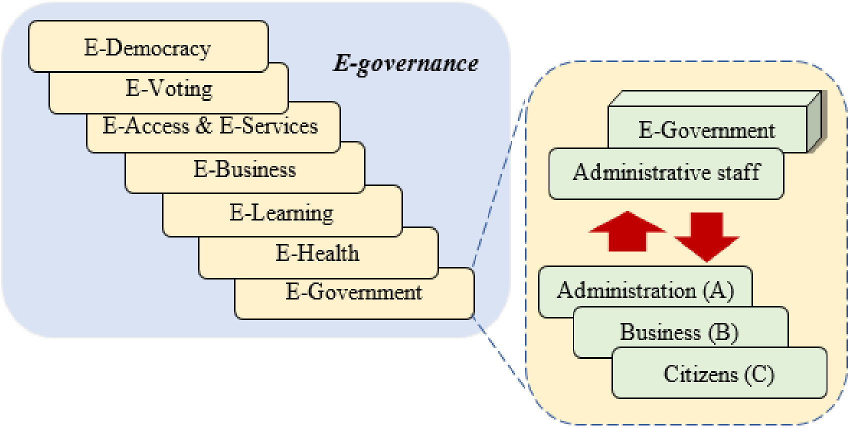


Fig. 2. Some basic components of e-governance

Figure 2 presents a statistic[2] for index rating of global regions based on E-Government Development Index (EGDI) for the year 2016. The index is based on three components: online service index, telecommunication infrastructure and the human capital index. The average value for the World is 0,49.

[2] https://www.statista.com/statistics/421584/egdi-e-government-development-index-region/

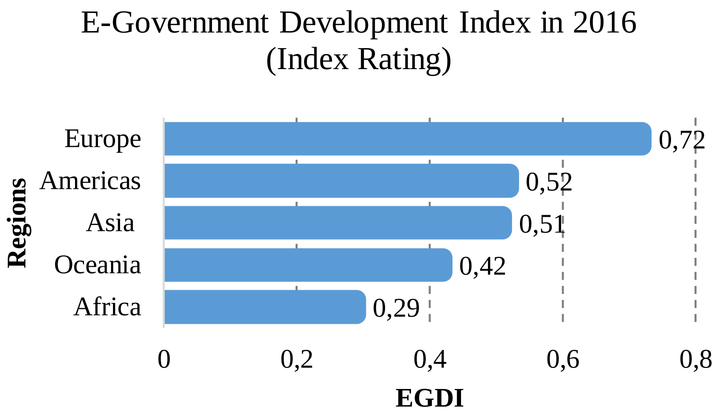


Fig. 3. Ranking of global regions based on EGDI

All components of the e-governance are realized by using contemporary ICT and they should be regarded as a structures and technologies for giving, storing, accessing and processing different types of information, including personal data. On the other hand, the internet usage of individuals increases. In this reason, e-government (as an example) is based on digital interactions between government structures and citizens, business and other governments. Different e-governments activities relate to information publishing, services, notifications, etc. that request answers of question and/or registration by uploading personal data. Other e-government transactions can require filling the fields with personal information. In this reason, the opportunities of e-governance (presented by the components) should be discussed in the frame of possible challenges for privacy and user's security.

Organization of e-learning environments.

The e-learning systems are distributed environments in the global digital world that propose services for education and training by internet transactions and information exchange. The extended version is so called Distributed Learning (DL) united principles of e-learning and networking. DL is an instructional model based on location of main participants and resources (instructors, teachers, students, system administrators, moderators, content, user's profiles, etc.) in different places in the global network and information servicing realization [19]. The uniting all distributed components could be realized by design of Distributed Learning Environment (DLE) based on adequate and effective conceptual model for distribution, sharing and accessing information and teaching materials, including using cloud storages. A solution for using smart technologies in e-learning is discussed in [3]. Other point of view is presented in [20]. The article determines that "*e-learning materials are critical in providing essential security measures to protect valuable data of users from vulnerable securities in materials*" and proposes a cloud based e-learning system which realizes two important aspects of information security – confidentiality and integrity. The goal of proposed system is "*e-learning materials in the cloud to be kept and secret*" and the elliptic curve cryptography algorithm is used for this goal. The presented in [20] architecture of cloud based e-learning system consists "*local server, centralized server and a web browser. In which multiple client* *will access their local server to upload or receive their material through internet. The learning material repository will consist of all learning material for the E-learners. The client will send a request to the cloud storage for the materials*". The basic modules of the proposed system are "accessing the document", "identifying possibility of attacks", "preventing attack" and "false positive attack verification".

The idea for using cloud services as a part of DLE activities could create some problems for data protection and user's privacy. A study of privacy control with audit of the e-learning processes based on cloud services is made in [21]. The goal of the authors is to present a concept "*of ensuring privacy to protect information shared between the e-learning system and cloud platform by proposing a mechanism to preserve the privacy of quite distinctive that supports public scrutiny on the information shared between these important technologies*". The uploaded by users own personal information could be protected by encryption mechanism based on AES encryption algorithm for protection of shared information.

Cloud services.

One of the main opportunities of the digital space is the cloud services that could be used based on multitenancy. In [22] is written "*The cloud service model intrinsically caters to multiple tenants, most obviously not only in public clouds but also in private clouds for large organizations* ". On the other hand, [6] declares "*In cloud environment, heterogeneity, uncertainty and dispersion of resources encounters problems of allocation of resources, which cannot be addressed with existing resource allocation policies*". An analysis of resource scheduling in cloud computing is presented in this article with a goal to help researchers in the process of selecting "*suitable algorithm for scheduling a specific workload*".

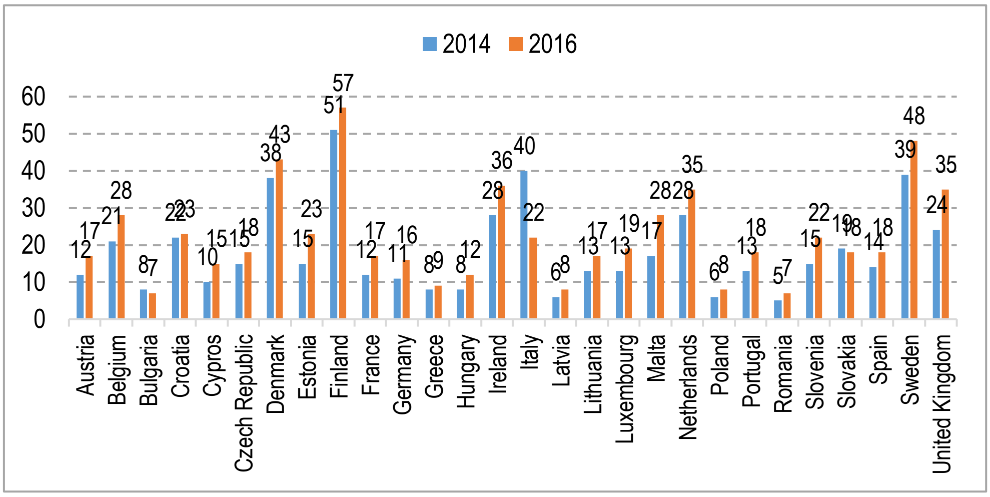


Fig. 4. Usage of cloud services over Internet [%] [3]
(average assessments for EU-28: year 2014 - 18,25%; year 2016 - 22,29%)

[3] Eurostat, Cloud computing services (Last update: 11-05-2017; visited October 2017) http://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do

If the term “cloud computing” is discussed two components should be analysed: cloud infrastructure (hardware and network resources for supporting proposed cloud services) and cloud software applications (system programs and applications that realize computing power for processing user’s requirements and running applications). The cloud services using increase and this is shown in fig. 4 for the enterprises of EU-28 countries. The difference between percentage for 2014 and 2016 is about 4%.

The enterprises with over 40% using cloud services during year 2016 are Finland (57%), Sweden (48%) and Denmark (43%), but there are countries with low level of using – Greece (9%), Latvia (8%), Poland (8%), Romania (7%) and Bulgaria (7%). On the other hand, the cloud services usage could be determined based on the type of the way for delivering by providers – public cloud (delivered from shared servers of providers) and private cloud (delivered from servers of providers exclusively reserved for the enterprise) – fig. 5 [23]. The figure shows that the large enterprises are used during 2016 more cloud services (45% total – 32% from public cloud and 24% from private cloud) in comparison with the small and medium enterprises (21% total – 15% from public cloud and 8% from private cloud).

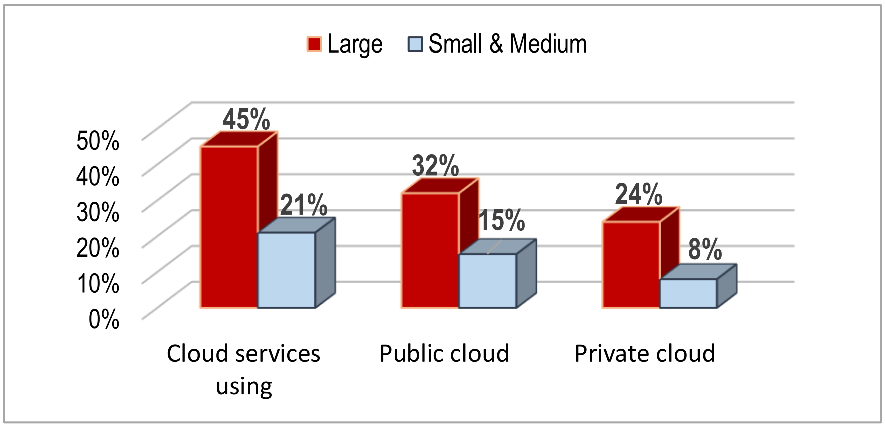


Fig. 5. Type of using cloud services for EU-28 delivered by different clouds

Hashem et al. [24] discuss another side of cloud computing – big data. They determine the cloud computing as “*a powerful technology to perform massive-scale and complex computing. It eliminates the need to maintain expensive computing hardware, dedicated space, and software”* and note the “*massive growth in the scale of data or big data generated through cloud computing*” The authors introduce in this article definition, characteristics, and classification of big data and determine that the addressing big data “*requires a large computational infrastructure to ensure successful data processing and analysis*”.

Another opportunity of cloud computing is so called “cloud manufacturing” introduced in [25]. The authors determine the cloud manufacturing as “*a new manufacturing paradigm as well as an integrated technology, which is promising in transforming today’s manufacturing industry towards service-oriented, highly collaborative and innovative manufacturing in the future*”. A critical review of the contemporary manufacturing technologies which permits to evaluate the proposed new side in the cloud environments is made in this paper.

Chang et al. [12] propose a cloud computing adoption framework (CCAF) “*to meet the requirements of business clouds and ensure that all implementations and services deliveries overcome all the technical challenges*”. The authors’ proposal is based on the conception that the security, trust, and privacy should be actual tasks at each system organization with cloud computing and big data. The business on the cloud has some important advantages at moving their data to the cloud and data centers – this permit to centralize the management of data centers, cloud services and applications. These opportunities reduce the cost for business processes organization and realization, and increase operational efficiency but could make some problems for user's privacy and personal data protection.

Social Computing.

What is the social computing? An acceptable vision of the social computing is that it collects different forms of social environments as social media, social *networks, social bookmarks, and social aggregators.* The Oxford Living Dictionaries[4] gives the following definition for the term social network: *"A network of social interactions and personal relationships" and in addition "an online community of people with a common interest who use a website or other technologies to communicate with each other and share information, resources, etc."*. Daniel Nations in [26] answer of the question "What is social media?" by determining the two parts – "social" (interacting with other people by sharing information with them and receiving information from them) and "media" (an instrument of communication) and proposes the following definition "*Social media are web-based communication tools that enable people to interact with each other by both sharing and consuming information".* The author asks in [26] very important question about the definition of the social computing: *"But if we use the term to describe a site like Facebook, and also a site like Digg, plus a site like Wikipedia, and even a site like I Can Has Cheezburger, then it starts to get more confusing. Just what is social media anyway*?". And finally, the article makes a conclusion that there is not a common understanding what must be determined as a social computing environment.

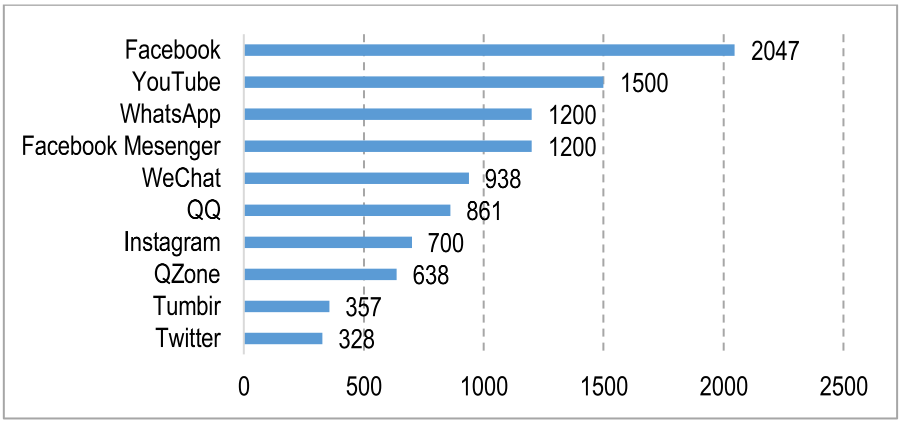
The components of the social computing (social media, social networks, blogs, etc.) are very popular and give useful opportunities for contacts and exchange of information between different users through the digital space [27]. This is valid not only for the individuals but also for business organizations, managers, traders, etc. There are different investigations for obtaining statistical assessments for using social network and media. For example, Fig. 6 presents two statistics determined by Statista (2017): (a) the top 10 of most popular social network sites worldwide as of August 2017; (b) number of countries using social media for e-consultation from 2010 to 2016. The last scheme shows that in 2016, 152 countries offered e-consultation through social media channels.

The index called Global Web Index (GWI) can present good statistics for the usage in the field of social computing. The report "The Social Media Trends to Watch in 2017"[5] examines the biggest trends dominating the 2017 social media landscape and gives some information about demographic distribution of the users, the work time for communications, most popular platforms, etc.

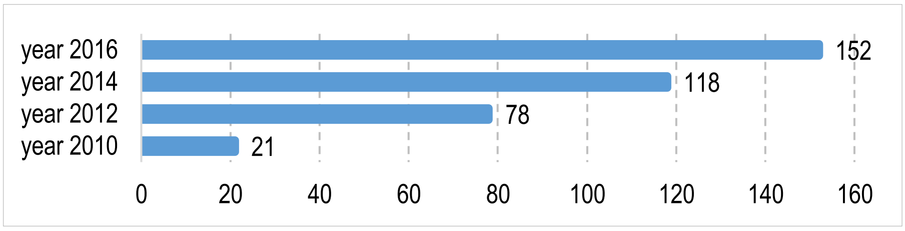
It is not secret that companies use social media for searching clients, staff, etc. On the other hand, the individuals upload their personal data to create a profile, but these data could be used by traders, managers, employers, etc. without permission of the data owner. This rises the ethical side and disturbs the principles of privacy and personal data protection.

[4] https://en.oxforddictionaries.com/definition/social_network

[5] http://insight.globalwebindex.net/social



(a) Most famous social network sites worldwide as of August 2017, ranked by number of active users (in millions) [6]



(b) number of countries using social media for e-consultation from 2010 to 2016 [7]
Fig. 6. Actual statistics determined by Statista, 2017

Internet of Things (IoT) and M2M communications.

Whitmore et al. [9] determine the IoT as "*a paradigm where everyday objects can be equipped with identifying, sensing, networking and processing capabilities that will allow them to communicate with one another and with other devices and services over the Internet to accomplish some objective*" and discuss the current state of research on IoT in [9]. Lin & Bergmann note in [28] that "*The European Commission has identified "Internet of Things" as one of its key work programs, supported by AIOTI - The Alliance for Internet of Things Innovation*[8]*. This consortium acknowledge that IoT will be responsible for future disruptive technologies ...*". In this paper authors discuss the application of IoT to the Smart Home and challenges to security and privacy. One of the remarks is about the need the IoT to be coordinated into a multi-vendor ecosystem.

It should be noted that the developing many IoT applications with different nature and characteristics creates three directions in this sector for increasing the opportunities of IoT architecture.

[6] https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (visited 25 September 2017)

[7] https://www.statista.com/statistics/421772/e-consultation-social-media/ (visited 25 September 2017)

[8] https://ec.europa.eu/digital-single-market/alliance-internet-things-innovation-aioti

Direction (1): Wireless sensor network (WSN) – it includes distributed sensors for monitoring physical parameters or parameters of the state of the environment. The data of this monitoring are sent via the network, which ensures processing and storing the information used for control of the other units in the system.

Direction (2): M2M communications (so called M2M model) ensure communications without human participation. This opportunity is based on the IoT architecture and permits to extend the services. M2M model is realized by smart systems, many active computers, sensors, and mobile unites for collection, sending, and processing monitored data. Application of the M2M model is to build smart cities, smart homes, smart networks, intelligent transport systems (for example see [29]), etc.

Direction (3): It is defined as an extension of the M2M-model for possible increasing information processing by using the new technologies and coordination between elements of the IoT-core. This direction is called "cyber-physical system".

The actualization of the M2M model is proved by the conclusion in [10] when is written "*Machine-to-Machine (M2M) communication is a promising technology for next generation communication systems. This communication paradigm facilitates ubiquitous communications with full mechanical automation, where a large number of intelligent devices connected by wired/wireless links, interact with each other without direct human intervention.*". In addition, the authors extend the area of application and add smart grids, e-healthcare, home area networks, and industrial automation. As a conclusion, the authors of [10] declare that "… *distinctive features in M2M communications form different challenges from those in human-to-human communications. These challenges need to be addressed, or otherwise it is not easy for this paradigm to gain trust of people.".* On the other hand, the number of IoT connected devices and M2M communications increase rapidly. For example, according the information by Statista, 2017[9] the increasing of the number of IoT connected devices worldwide from 2015 to 2017 is over 32% with a prognosis for 3,7 times increasing from 2017 to 2025. Other statistical data[10] present 1,8 times increasing of the number of M2M connections worldwide from 2017 to 2020. Finally, Brittany Dervan presents in [30] "17 stats that shows the massive opportunities of IoT".

It should be noted that the opportunities of IoT, M2M, Smart Home/Smart City determine challenges for security and privacy. The authors of [28] determine that "*many of the principles applied to safety critical systems and enterprise security are equally applicable to IoT security*" and note three main themes: confidentiality, authentication and access. US Departments of Homeland Security has published on 15 November 2016 "Strategic Principles for Securing the Internet of Things (IoT)" [11], presented below.

✓ Incorporate Security at the Design Phase.
✓ Promote Security Updates and Vulnerability Management.
✓ Build on Recognized Security Practices.
✓ Prioritize Security Measures According to Potential Impact.
✓ Promote Transparency across IoT.
✓ Connect Carefully and Deliberately.

[9] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[10] https://www.statista.com/statistics/487280/global-m2m-connections/

[11] https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

4. PRIVACY AND INDIVIDUAL'S RIGHTS

Many of the discussed upper opportunities create challenges for user's privacy and personal data uploaded in the digital social environments or stored data in cloud, data centres, etc. Some of these challenges are discussed in this section.

Chang et al. [12] determine that the system design and deployment must be made based on the principles of "*current security practices*". The goal must be protection of user's privacy and confidentially, integrity, and availability of data. In this reason, it is very important to develop a suitable framework for integration of the resources on the base of guidelines, policies, standards, and rules for user's security and privacy. The authors cite some research in this field as 'Usage-Based Security Framework' (UBSF) for collaborative computing systems, 'TrustCloud framework' which is focused on accountability, 'comprehensive security framework', 'wireless sensor networks model', etc., but "… *there are no details on the actual use of the proposals and also no clear evidence of adoption of these proposals to business clouds*". In this direction, the proposed in [12] CCAF is used for developing cloud storage, bioinformatics solution, and authorized access to the resources. This permits development of guidelines for financial modelling, best practices, and change the risk.

The free information moving and remote access to knowledge, learning, information and other resources create several challenges for privacy and user's rights protection. Haggard & Jablonski [31] write that "*free flow of information creates markets by exposure to intellectual properties, while copyright secures economic benefit to copyright holders from the flow"* and in addition write "*All knowledge regulation policies involve balancing access and restriction*". On the other hand, Bode & Jones [32] discuss the proposed new paradigm so-called "right to be forgotten" and they determine it as "*a legal right that allows citizens to petition to have information about them taken down from the Internet*". The authors investigate in this paper the problems of privacy in the information age and conclude that "*the law should apply only in minors*".

The same problems could be determined in all digital environments and technological structures in the digital world, supported social computing, distributed mobile e-learning, e-governance realizations, IoT, M2M communications etc. In this reason, Kelvin Claveria confirms in the on-line publication "13 stunning stats on the Internet of Things", 28 April 2017 (https://www.visioncritical.com/internet-of-things-stats/) the information presented by Statista 2017 with the comment that "*in 2015, there were about 15,4 billion connected devices and this number will grow to 30,7 billion in 2020, and 75,4 billion by 2025*". The author writes that some of the used units as industrial sensors, connected manufacturing machines, in-store analysis devices and workspace management applications are already on the market and concludes "*These B2B IoT devices will fundamentally transform the way organizations do business with other companies*". On the other hand, the collection and analysis of data from connected devices for identifying human location, devices status and connections will increase – for example for 2017 the part of global manufacturers that use analytics data is about 60%.

Summarization of the main problems of privacy and security in a connected world, and personally in IoT, is made in [33]. This FTC Staff Report discusses the benefits and risks, application of traditional privacy principles and legislation. Another point of view for privacy and security challenges is presented in [28].

A summary of the main challenges of digital spaces which could disturb the user's security and privacy are presented below.

(1) The legislation in the field of privacy and PDP determines three categories of persons which take part in the personal data processing – data controller, data processor and data subject. The right over the personal data has the data subject which is an owner of the personal data. On the other hand, the Directive 95/46/EC determines as an obligation of the data controller defining the goal for personal data processing and the processed categories of personal data. It is very difficult to control these obligations because at several digital environments is impossible to specify what is the role of each participant at communications (data subject, data processor or data controller), because the functions of customer, vendor and provider and the relation between them could be defined for specific case only. In addition, the service providers have no legal obligation to protect personal data if they are not defined as data controllers or data processors. In this reason, the new European document *General Data Protection Regulation (GDPR)* has been accepted and will come into force in May 2018.

(2) The users with a role of "data subject" (owner of his/her data) have many rights and providers and vendors must protect their personal data collected during the registration procedure and/or during the communications. The first step before starting personal data collection and processing is determining the goal. There are cases for extension of the set of categories of required personal data which must be uploaded in the created profile (for example, names, birth date, address, phone number, social life, gender, country, hobbies, relationships, etc.). This data collection needs restriction and regulation.

(3) The data protection law permits revision by the data owner of all personal data uploaded in his/her profile. The data subject can make access to own data, blocking of incorrect data and delete these data that are not valid, not actual or are not used yet. Data controller must guarantee that each user could define restriction for the own profile accessing. This will prevent unauthorized access and incorrect dissemination of personal information. This action could be realized by making the profile private from the user by selection of the people who can visit the page and to restrict all accesses by using authentication procedure.

(4) Another right of the data subject is to demand deletion of several or all personal data in the profile if the goal is realized (personal data must be canceled at a refusal of environment/service using). The problem is that if any user wants deletion of her/his own data from the personal profile he/she will be not sure that these data are really deleted. The reason is that the data are often transferred to other places in the digital space and there not guarantee that all copies of the data in these places (nodes) have been really deleted. This problem could be extended with the case of transfer of personal data to third party before required deletion. In this case the destination place will keep the received copy of data and the user will not be aware of that. This will be a problem of privacy for the individual. Data protection legislation gives strong rules for deletion of personal data in the traditional cases, but for the digital spaces (cloud, social environments, mobile network communications, e-business sites, etc.) this is not clearly determined.

(5) The information sharing between potential unknown users could be determined as another challenge for individual's privacy and security. It is well known that sharing information is traditional activity for the network society, but this information (including, for example, and sensitive personal data) could be accessible by unknown users from different places of the world. This could cause serious problems as data loss, integrity destroying, problems with accountability, hackers' attacks, etc. In these cases, the data owner does not know what IT security policy and measures are used for counteraction to eventual attacks.

(6) The next challenge for privacy is the data transfer to other countries and this country must have a PDP-level that is adequate to this in the EU countries. There is a practice the

data to be transferred to different locations in different countries, for examples for storing data (data centers, cloud infrastructure), between service providers (social media), changing information between collaborators, etc. A request of data protection low is the owner of data to be informed for all transfers of their data.

(7) And finally, another important obligation for all data controllers (providers, vendors, etc.) is to implement appropriate measures for information security and to protect user's privacy. Who will check and control if this obligation is respected? Can the user determine what measures are implemented? Can he/she oppose to illegal access to the information resources and/or unauthorized using private information or personal data? All service providers must guarantee an effective protection of data integrity and data availability in supported digital environment.

Based on the discussed problems for individual's privacy a strong regulation of accessing all information resources and personal data must be organized based on technological and technical means and tools. Fig. 7 shows a proposal for organization of System for Information Security Management in a distributed structure that uses three types resources – public resources (with free access and using); internal resources (stored in own memories and data structures); external resources (stored in data centers or in the cloud components). The personal data could be organized as internal and/or external information resources. The main components of this SISM are registration, identification, verification, authentication and authorization, used in different places after preliminary analysis.

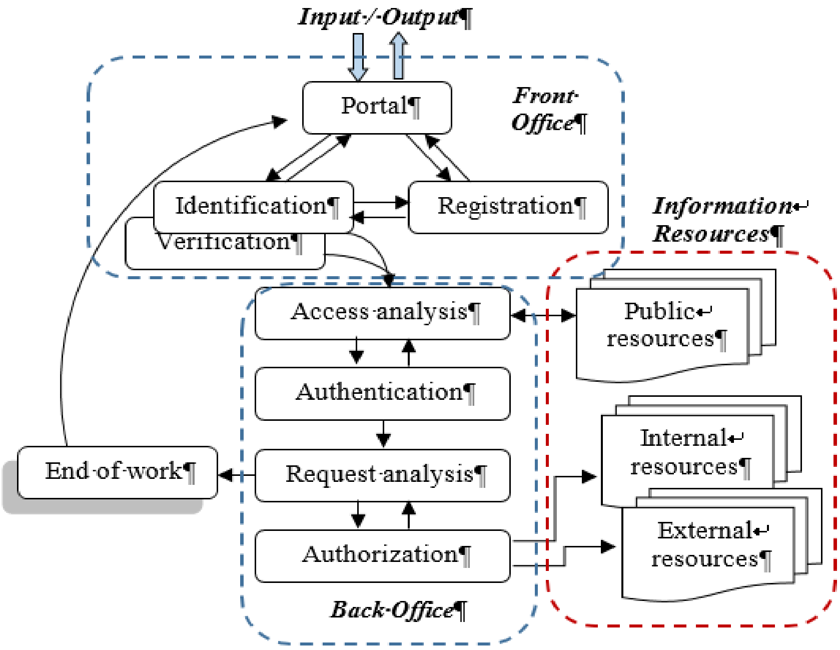


Fig. 7. Organization of System for Information Security Management (SISM)

5. CONCLUSION AND FUTURE WORK

The first part of the article presents a survey of some opportunities of the digital spices organized as heterogeneous environments based on contemporary technologies as cloud and social computing, e-services and e-management, IoT and M2M, etc. The second part discusses important challenges for user's security and privacy. These challenges are determined on the base of European directives and the rules for data protection and their extension in the point of view new processes in the cyberspace. These challenges define several problems which must be decided for securing privacy of individuals as users of the network services.

As a future work, a suitable organization of procedures for secure access and privacy protection could be developed. These procedures should be realized in a united environment which combines traditional infrastructure (own processors and storages) and components of the digital world (cloud, data centers, social networks & media, etc.). This heterogeneous environment must secure adequate identification, verification, authentication and authorization.

ACKNOWLEDGMENTS

This research has been made with support of project DH-07/10 funded by Bulgarian Ministry of Education and Science.

REFERENCES

[1] Ojha, S. I. Pandey. Management and Financing of e-Government Projects in India: Does Financing Strategy Add Value? *IIMB Management Review*, No. 2 (vol. 29), June 2017, pp.90-198. doi.org/10.1016/j.iimb.2017.04.002. Available at: http://www.sciencedirect.com/science/article/pii/S0970389617302033

[2] Elkadi, H. Success and Failure Factors for e-Government Projects: A Case from Egypt. *Egyptian Informatics Journal*. No. 2 (vol. 14), July 2013, pp.165-173. doi.org/10.1016/j.eij.2013.06.002. Available at: http://www.sciencedirect.com/science/article/pii/S1110866513000236

[3] Hedvicakova, M., L. Svobodova. Use of Smart Technologies in the e-Learning Course Project Management. In the book *"Smart Education and e-Learning"* (ed. V. Uskov et al), 2017, Springer International Publishing, 2017, pp. 167-176. Available at: https://books.google.bg/books?id=SY-olDwAAQBAJ&pg=PA167&lpg=PA167&dq=projects+in+e-learning+2017&source=bl&ots=GdbWc5dHd2&sig=jw4h7Xl-tIW6LGVnBNXgMMhVyHg&hl=bg&sa=X&ved=0ahUKEwj61c_37KvWAhXC6RQKHVy5DX04ChDoAQgrMAA#v=onepage&q=projects%20in%20e-learning%202017&f=false

[4] Doneva, R., S. Gaftandzhieva, G. Totkov. FETCH Project: The Maturity of Quality Management Through Dynamic Evaluation of the Project Progress. *International Journal on Information Technologies and Security*, ISSN 1313-8251, No. 3 (vol. 8), September 2016, pp. 29-38. Available at: http://ijits-bg.com/ijitsarchive

[5] Elysium Technologies Private Limited. 2016-2017 Final Year Projects: Cloud Computing – Titles and Abstracts, 2017. Available at: http://elysiumtechnologies.com/2016-2017-final-year-projects-cloud-computing/

[6] Singh, S., I. Chana. A Survey on Resource Scheduling in Cloud Computing: Issues and Challenges. *Journal of Grid Computing*, Vol. 14, No. 2 (vol. 14), June 2016, pp. 217-264.

[7] *Social Computing and Social Media. Applications and Analytics* (ed. G. Meiselwitz), 9th International Conference, SCSM 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings, Part II, Springer, eISBN 978-3-319-58562-8, 469 p. doi: 10.1007/978-3-319-58562-8. Available at: http://www.springer.com/gp/book/9783319585611

[8] Ngai, E. W. T., S. S. C. Tao, K. K. L. Moon. Social media research: Theories, constructs, and conceptual frameworks. *International Journal of Information Management*, No. 1 (vol. 35), 2015, pp. 33-44.

[9] Whitmore, A., A. Agarwal, L. D. Xu. The Internet of Things – A survey of topics and trends. *Information Systems Frontiers*, No. 2 (vol. 17), 2015, pp. 261-274.

[10] Verma, P. K., R. Verma, A. Prakash et al. Machine-to-Machine (M2M) communications: A survey. *Journal of Network and Computer Applications*, Vol. 66, May 2016, pp. 83-105.

[11] Acquisti, A., L. Brandimarte & G. Loewenstein (**2015**). Privacy and Human Behavior in the Age of Information. *Science*, No. 6221 (vol. 347), 2015, pp. 509-514.

[12] Chang, V., Y-H Kuo, N. Ramachandran. Cloud Computing Adoption Framework: A Security Framework for Business Cloud. *Future Generation Computer Systems*, Vol. 57, 2016, pp.24-41.

[13] Ali, M., S. U. Khan, A. V. Vasiliakos. Security in Cloud Computing: Opportunities and Challenges. *Information Sciences*, Vol. 305, June 2015, pp. 357-383.

[14] Fischer, A. E. Improving User Protection and Security in Cyberspace, *Report of Committee on Culture, Science, Education and Media*, Council of Europe, 12 March 2014. Available at: http://www.statewatch.org/news/2014/mar/coe-parl-ass-cyberspace-security.pdf

[15] Aced Félez, E. The Proposal of the European Commission for a Data Protection Directive in the Police and Criminal Justice Field. *International Journal on Information Technologies and Security*, No. 2 (vol. 7), June 2015, pp. 37-58. Available at: http://ijits-bg.com/ijitsarchive

[16] Romansky, R., I. Noninska. Architecture of Combined e-Learning Environment and Investigation of Secure Access and Privacy Protection. *International Journal of Human Capital and Information Technology Professionals*, No. 3 (vol. 9), 2016, pp. 89-106.

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

[18] Kim, H. E-learning Privacy and Security Requirements: Review. *Journal of Security Engineering*, No. 5 (vol. 10), 2013, pp. 591-600.

[19] Romansky, R. *Information servicing in distributed learning environments*, Saarbrüken, Germany, LAP LAMBERT Academic Publishing, 2017 (100 p.).

[20] Lavanya, N. A., M. Buvana, D. Shanthi. Detection of security threats and vulnerabilities of e-learning systems in cloud computing, *Advances in Natural and Applied Sciences*, *11*(7), 2017, pp.550-559.

[21] Al-Khafaji, K. M. K., Eryilmaz, M. Auditor technology and privacy control to secure e-learning information on cloud. In *Proceedings of International Conference on Progress in Applied Science*, Istanbul, Turkey, 2017.

[22] Tang, B., R. Sandhu, Qi Li. Multi-tenancy Authorization Models for Collaborative Cloud Services. *Concurrency and Computation: Practice and Experience*, No. 11 (vol. 27), 2015, pp. 2851-2868.

[23] Giannakouris, K., M. Smihily. Cloud computing - statistics on the use by enterprises, Eurostat Statistic Explained, December 2016, available at: http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises
(visited at 25 Sept 2017)

[24] Hashem, I. A. T., I. Yaqoob, N. B. Anuar et al. The Rise of "Big Data" on Cloud Computing: Review and Open Research Issues, *Information Systems*, No. 1 (vol. 47), 2015, pp. 98-115.

[25] Ren, L. et al. Cloud manufacturing: Key Characteristics and Applications. *International Journal of Computer Integrated Manufacturing*, No. 6 (vol. 39), 2017, pp. 501-515 http://dx.doi.org/10.1080/0951192X.2014.902105

[26] Nations, D. What Is Social Media? Explaining the Big Trend. Take a closer look at what 'Social Media' is really all about, *Lifewire*, 30 May 2017, available at: https://www.lifewire.com/what-is-social-media-explaining-the-big-trend-3486616

[27] Romansky, R. Social Media and Personal Data Protection. *International Journal on Information Technologies and Security* (ISSN 1313-8251), Vol. 6, No 4, Dec. 2014, pp.65-80.

[28] Lin, H., N. W. Bergmann. IoT Privacy and Security Challenges for Smart Home Environments. *Information*, 7, No. 3, 2016, 15 p.; foi:10.3390/info7030044, http://www.mdpi.com/2078-2489/7/3/44/htm (accessed on 3 Oct. 2017)

[29] Ivanova, Y. Modelling the Impact of Cyber Threats on a Traffic Control Centre of Urban Auto Transport Systems, *International Journal on Information Technologies and Securit*y, No. 2 (vol. 9), 2017, pp. 83-95.

[30] Brittany Dervan, *17 Stats that Show the Massive Opportunities in the Internet of Tings*, 2 March 2017, available at: http://blog.skyhookwireless.com/iot/internet-of-things-statistics

[31] Haggart, B., M. Jablonski. Internet Freedom and Copyright Maximalism: Contradictory Hypocrisy or Complementary Policies? *The Information Society. An International Journal*, No. 3 (vol. 33), 2017, pp. 103-118.

[32] Bode, L., M. L. Jones. Ready to forget: American Attitudes Toward the Right to be Forgotten. *The Information Society*, No 2 (vol. 33), 2017, pp.76-85

[33] Internet of Tings – Privacy and Security in a Connected World. FTC Staff Report, January 2015, available at: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Information about author:

Radi Romansky is full professor at Technical University of Sofia, Department of Informatics, Ph.D. in Computer Engineering and D.Sc. in Informatics and Computer Science; Vice Rector of Technical University of Sofia; Full member of European Network of Excellence on High Performance and Embedded Architectures and Compilation (HiPEAC). He has been a member of Bulgarian Commission for Personal Data Protection (2002-2007). Areas of scientific interests: ICT, informatics, computer architectures, computer modelling, data protection, etc.

Manuscript received on 04 October 2017