The North African Journal of Scientific Publishing (NAJSP)
مجلة شمال إفريقيا للنشر العلمي (NAJSP)
E-ISSN: 2959-4820
Volume 2, Issue 4, October - December 2024
Page No: 249-254
Website: https://najsp.com/index.php/home/index
SJIFactor 2024: 5.49 معامل التأثير العربي (AIF) 2024: 0.71 ISI 2024: 0.696

Developing Specific Specifications for User Security and Privacy Protection Through Cyberspace Features

Elmakzum Kamis Elmakzum Elgedik *
* Department of Computer Science, Faculty of Science, Bani Walled University, Bani Walled, Libya

تطوير مواصفات محددة لأمن المستخدم وحماية الخصوصية من خلال ميزات الفضاء الإلكتروني

المخزوم خميس المخزوم الجدك *
*قسم علوم الحاسوب، كلية العلوم، جامعة بني وليد، بني وليد، ليبيا

*Corresponding author: almakzoumaljedk@bwu.edu.ly

Received: October 03, 2024	Accepted: November 20, 2024	Published: December 23, 2024

Abstract

The paper discusses a few issues that have emerged in the modern digital era and are strongly related to the gathering, using, and sharing of user data. The discussion is based on a brief explanation of modern cyber technologies and elements of the digital era connected to user privacy. The main issues facing the internet are compiled, and certain specifications for user security and privacy protection are developed.

Keywords: Digital age; Cyber technologies; Privacy; Data protection, User's security.

الملخص

تتناول هذه الورقة بعض القضايا التي ظهرت في العصر الرقمي الحديث والتي ترتبط ارتباطًا وثيقًا بجمع واستخدام ومشاركة بيانات المستخدم. وتستند المناقشة إلى شرح موجز لتقنيات الإنترنت الحديثة وعناصر العصر الرقمي المرتبطة بخصوصية المستخدم. ويتم تجميع القضايا الرئيسية التي تواجه الإنترنت، وتطوير مواصفات معينة لأمن المستخدم وحماية الخصوصية.

الكلمات المفتاحية: العصر الرقمي، تقنيات الإنترنت، الخصوصية، حماية البيانات، أمن المستخدم.

Introduction

The use of information and communication technology (ICT) in various areas of public and social life is the foundation of our society's current stage [1] discusses the significance of "being inventive and competitive in today's global digital economy. Social communication, information sharing, remote access to various distant resources, data collection, etc. are the main activities of the digital era. This has to do with invading the personal privacy of those people who participate in networked activities and calls for strict regulation over how personal data is used and protected [2]. For this reason, the European General Data Protection Regulation (GDPR) [3] has established a fundamental framework for maintaining user privacy as well as strict regulation of the collection, use, and dissemination of their personal data provided at the time of registration and/or during the service [4, 5]. The processing of genetic data is described in [5], where it is noted that privacy policies must be created and that the security of these data is crucial because they include sensitive information. This article's goal is to provide a concise summary of some fundamental standards for protecting user privacy and personal information while it is utilized online. In the second section, a quick overview of the Information Society (IS) and its fundamental components is made in order to achieve this purpose. The third section examines the most important cyberspace technologies, including big data and big data analysis [8, 9], cloud computing (CC) and mobile cloud computing (MCC) [6, 7], and Internet of Things (IoT) in its various forms [8], The following two parts address various issues relating to user privacy and the establishment of standards for technologies used in cyberspace.

Digital Space Features

The Information Society (IS), which embraces information as a basic good with the aim of elevating individuals' status (economic, cultural, social, educational, etc.) through the use of modern ICT, presents the unique characteristics of the digital age.

Historical Aspects of the IS Creation

The words "information society" were first used in a written document by the editors Michiko Igarashi and Jiro Kamishima in January 1964 [10]. The Information Society: From Hard to Soft Society by Yujiro Hayashi and Introduction to an Information Society by Yoneji Masuda and Konichi Kohyma, both published at the end of the 1960s, have both examined this concept. The inclusion of the phrase in the Japanese lexicon Johoka Shakai Jiten, lexicon of Information Societies, in 1971 gave it official recognition as a component of information technology. The phrase "knowledge base industry" was first used by Fritz Machlup to describe the processes of enhancing the role of information and knowledge in public life and industry in 1962. In the following two decades (1970s and 1980s), other descriptions are put out, including "post-industrial society," "postmodern society," "information economy," "information revolution,"white colour revolution," "network society," etc. The transition from the industrial to the information society can be defined in the simplest possible way by using the definition of the former society while changing the type of services provided: "The transition from the industrial to the new information society is realized if over 50% of the people are employed in the sphere of information-intellectual services. For this reason, it may be said that the term "information society" is still valid today. It refers to a society where information technology (ICT) predominately supports, presents, and disseminates knowledge across a global network.

Basic Features of the Information Society

The major objective of an information society, which views information as a basic good, is to use ICT to raise people's economic, social, and cultural standing. It can be concluded that expanding the role of distributed information resources in the global network at the turn of the twenty-first century marks the beginning of the complete realization of IS principles. Below are a few of the I's fundamental characteristics.

1- Essence: A civilization in which knowledge and information are the main products12-The goal is to use ICT to enable efficient data sharing and quick connections across institutions.
2- Creating virtual environments modeled after actual physical devices, businesses, warehouses, etc. is known as virtualization
1. Integration is the process of developing a new type of networking by integrating distinct network components as stand-alone modules for service delivery.
2. humanization, the process of establishing a "society without frontiers" to create a new, uniform unity among all cultures.
3. Globalization is the ability of society to collaborate without boundaries in terms of time and space, allowing for the simultaneous completion of individual and global tasks by various actors in various locations.
4. Dynamics: fast information updates, electronic communications, and a shorter production life cycle are all part of real-time operations.
5. The fundamental force behind society and business is innovation, which includes creative tactics, approaches, and endeavors.

The primary objective of the IS might be ascertained based on the key characteristics mentioned above. By integrating various components, it is intended to establish an appropriate and effective information environment and systems that enable contemporary management and remote access to information resources located in various network nodes. The cyber technologies of the current digital era may aid in the resolution of this worldwide task. The two main components of this collaboration are as follows:

1- The technical equipment, information items, applications, specialized programme tools, metadata, and descriptors that are used to manage remote access and processing are all considered information resources.

2- Information security is a collection of policies, guidelines, and instruments for guaranteeing the trustworthy safeguarding of information assets against inaccurate, unlawful, or unauthorized access that could contaminate or destroy data or system components (hardware and software.

Cyber Technologies and Privacy

Modern digital space technologies and applications, such as social computing, cloud and mobile cloud services, Internet of Things (IoT) with stages for machine-to-machine (M2M) communication and cuber-physical systems (CPS), big data analysis, etc., enable the expansion of the role of information systems (IS) into both personal and professional spheres. Each of these technologies creates unique sectors that are dynamic and provide new challenges for human privacy [11].

Social networking sites (SNS), which include social media, social networks, social bookmarking social aggregators, blogs & micro blogs, wikis, multiplayer games, etc., are the environments that make up social computing (SoC), which is interactive communication between different individual users in the worldwide network. The SoC is a useful tool for information sharing and communication, but because the information is shared with so many other users, even those who are not known to them, there is a risk to the privacy and personal data of the users [12-15]. However, the information gathered and kept at the initial user's Transferring a registration to a different virtual space node was possible.

Cloud computing is a distributed environment-based technology that assembles virtual computers, storage's, and other components with dynamic communications between them to provide users with a variety of services. The privacy of users is unrelated to cloud services; however, they may be tied to international data transfers that include personal information. This might go against GDPR rules governing the safety of personal data and how it is transferred between multiple cloud locations. For this reason, specific precautions for cloud-based shared data protection should be considered [13].

The term "Internet of Things" (IoT) refers to a collection of items and gadgets that are linked to the Internet and used to send and receive data gathered from the sensor-based monitoring of particular parameters. IoT unifies rules, protocols, standards, and applications for managing the connection with devices and sensors, ensuring remote control of the parameters being monitored, in order to achieve this goal. In the article [7], the relationship between processes' success and IoT framework characteristics is discussed. To demonstrate this dependence, a survey of a few security concerns relating to IoT frameworks with various architectural styles is conducted.

The findings demonstrated that alternative approaches might give security features even when the same standards for communications were used.

IoT indicates a trend of increasing usefulness and its importance in people's daily lives. This describes the importance of the methods for protecting user privacy and the need to offer trustworthy information security. In this regard, Figure 1 depicts a general layout of the key IoT components.

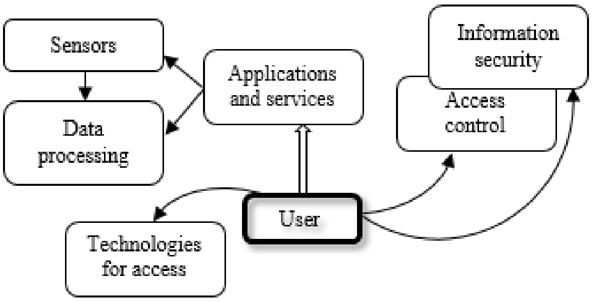

Figure 1: Formal description of relations between components in IoT.

Big data are systems that gather and store enormous amounts of information from several sources. Big Data Analysis (BDA), a technology for processing and analyzing massive volumes of data for any purpose, is linked to this phrase [8]. This analysis is crucial for research in fields including industry, health, and education, especially for organizations where the knowledge gathered has a marketable value. This article examines the potential "more complex and difficult to manage" security issues with big data analysis as well as the potential disruption of individual privacy [9]. The main privacy issue with BDA is how the results are interpreted, which might lead to privacy violations if the monitored object is a person.

Challenges for Security and Privacy

Information exchange and remote access to global network resources are the foundations of the digital world. The users group $U = \{U1, U2, UN\}$ $(U \neq \varnothing)$ access a variety of settings' chosen dispersed resources $IE = \{IE1, \ldots IEM\}(IE \neq \varnothing)$

Each environment is assumed to have its own technological components for the information service's structure, such as a preregistration module and a database (DBforPD) where users' personal data (PD) is collected as illustrated in Figure 2.

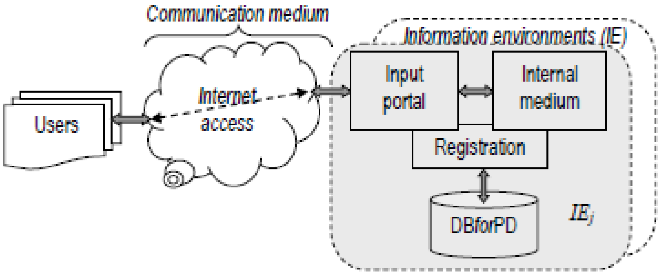

Figure 2: Remote access to information resources.

In reality, every user has the ability to transport or access data—including personal data—over national boundaries and throughout the globe via the network. Because it is possible to violate digital privacy (e-privacy), this can be classified as a cyber spice mining problem. During the early registration process, numerous network environments typically involve the input of personal data in categories that are outside of the specified purpose. According to a study, more than 74% of EU residents think that sharing personal information is a standard practise in the modern digital age.
The registration asks for the provision of specific PD categories that the IE-owner stores and processes. The following queries come up:

1- Where and how are these personal records kept? Which laws apply to them, and who has access to them?
2- Who is responsible for safeguarding users' private data and for creating measures to prevent data alteration or deletion?
3- Which regulations need to be followed in order to store private information and maintain confidentiality when using digital platforms?
4- How might one ensure the accuracy of the transfer of personal data across various global network nodes and its integrity?

The following themes will examine the answers to these and other questions:

1- Are personal data on social networks protected?
2- What is the fate of personal data stored in the cloud?
3- Are there privacy issues with the Internet of Things?
4- Is privacy safeguarded during Big Data analysis?
5- How can one ascertain the identity of a “Data Controller” and identify the most appropriate law enforcement method?

The current state of cyberspace challenges the conventional understanding of privacy, which was defined as "the right to be alone" (first presented by Samuel D. Warren and Louis Brandeis in their 1980 article "The Right to Privacy") and replaces it with the new understanding of "the right to be forgotten/to be erased," which is a primary paradigm included in the GDPR. For this reason, companies that offer various information resources and distribute services via the Internet are required to notify users about privacy policies, which include guidelines, procedures, and technological resources and tools for processing and protecting personal data in an appropriate manner. It is a reality that a large number of users consent to the privacy policies upheld by the relevant network area without realizing it. There are instances where there is insufficient information about how to process, store, and give user personal data to a third party. The user registers since they are left with no other option. Additional cases relate to missing policy information on the accessed website (portal) or to the registration process requiring personal data categories unrelated to the services and objective supported. The following list includes some categories of personal data that are gathered when a user registers and uses a social network.

1- Name, previous and email addresses, date of birth, phone number, fax number, detailed information about hobbies and interests, friends, and other details are needed for registration and profile updates
2- When working or accessing, information about the visit, such as the date and time of access, IP address, kind of browser, sites visited, location, and device type (if using a mobile phone) is collected.

Security And Data Protection Requirements

Effective execution of legislative and technical standards, as well as full interaction between individuals, businesses, and administration, are crucial to resolving these potential privacy issues. Strong information security, data protection, and privacy preservation must be the goals of all these regulations. For instance, multi tenancy in the cloud offers a shared virtual environment for numerous users, which may lead to the security issues listed in Table 1.

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 storage's organization
	▪ Unprotected web applications using
	▪ Weak access control
	▪ Bad digital right management
Contract aspect	▪ Unsecure servicing and dissemination
	▪ Illegal personal data dissemination

Because multiple users can share a single programme or application and access stored data via mobile devices, multi-tenancy systems pose significant security challenges. This puts confidentiality at risk and necessitates strict supervision, which includes authorization and personal identity. Every degree of security needs to be carried out, and Figure 3 shows how a System for Information Security (SIS) is organized for this purpose.

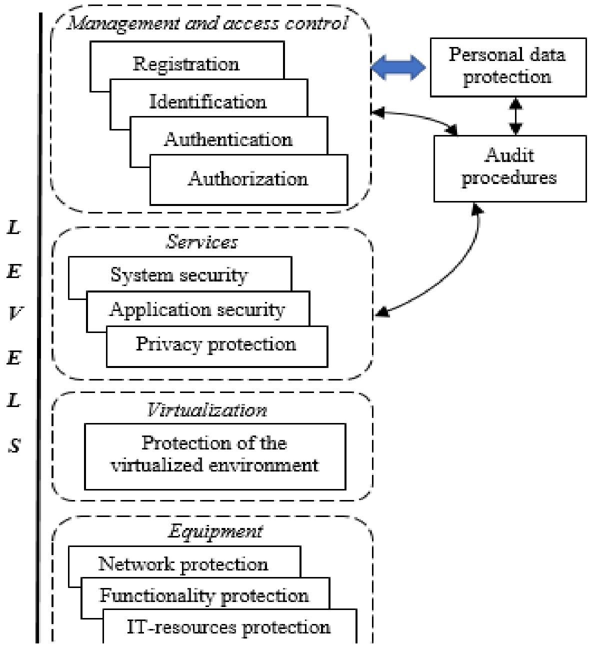

Figure 3. Security organization to protect resources in cloud services.

It is crucial to stress that network and device security are not the only aspects of IoT security. It is important to take into account every element, such as USB ports, cloud, mobile apps, software, and network interfaces. For this reason, the following significant IoT requirements could be identified.

1. Once items are identified, their connectivity has to be understood.
2. It is necessary to guarantee interoperability between various systems that communicate with each other.
3. To ensure exact network functionality and automated data processing, autonomous networking and servicing are necessary.
4. Because every "thing" works with data that can be treated for confidentiality, authenticity, and integrity of data, including personal data, security is a crucial necessity for the Internet of Things.

5. Because the Internet of Things is connected to many aspects of daily life, sensitive personal information about people is gathered and processed. As such, privacy protection should be considered in this context.

All phases of the process, including data transmission and collecting, aggregation, storage, mining, processing, and analysis, must be able to accommodate this requirement. Similar questions can also be raised about social computing and the primary recommendation, which needs to deal with the necessary information with the utmost accuracy. Users must have a decent chance to learn about any privacy violations in a timely manner. Everyone ought to be aware of the types of personal data that will be handled.

Conclusion

The protection of integrity (against unauthorized deletion, modification, or theft) and availability (access to services, data, and resources wherever and whenever) can be summed up as the primary needs for information security in cyberspace. The GDPR regulation outlines the "right to be forgotten" paradigm, which calls for wiping all personal data after processing purposes are completed, and "privacy by default," which states that default settings should maximize privacy. These concepts help identify the criteria for data protection.

Reference

[1] 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

[2] 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

[3] 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, vol. 3, No. 3, 2018, pp.2096-2100; available at: http://ijsrcseit.com/paper/CSEIT18354.pdf

[4] 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.

[5] D. Ivanova and A. Elenkov, “Big Data Analytics for air quality monitoring assessment based of IoT platform”, International Journal on IT and Security, vol. 11, No. 2, 2019, pp.43-50.

[6] 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.

[7] W. G. Voss. “European Union data privacy law reform: General Data Protection Regulation, privacy shield, and the right to delisting”, Business Lawyer, vol. 72, No. 1, Jan 2017, pp. 221-233.

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

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

[10] 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

[11] W. Van Grembergen, and St. De Haes, “Introduction to the minitrack on IT governance and its mechanisms”, Proceedings of the 51st Hawaii International Conference on System Science, 2018, pp. 4877-4879; available at: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1578&context=hicss-51

[12] M. Khaleel, A. A. Ahmed, and A. Alsharif, “Artificial Intelligence in Engineering,” *Brilliance*, vol. 3, no. 1, pp. 32–42, 2023.

[13] 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.

[14] M. Khaleel, A. Jebrel, and D. M. Shwehdy, “Artificial intelligence in computer science,” Int. J. Electr. Eng. and Sustain., pp. 01–21, 2024.

[15] 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, available at: https://www.tandfonline.com/doi/abs/10.1080/1369118X.2018.1486870