Internet of Thongs and User Privacy Protection

Radi Romansky
Technical University of Sofia (Bulgaria)

Contents

Abstract

The object of this article is to discuss the features of the digital world based on the global network space and contemporary information technologies, in particular ше Intern of Things (IoT). A brief survey of main types of information with specifying the place of the personal data is made in the introduction. Social aspects of the Internet space are discussed whit determining the negative consequences for privacy. The features of IoT including short presentation of the important versions (wireless sensor networks, machine-to-machine communication, and cyber-physical systems) are presented. And finally, the challenges of IoT for the user privacy and personal data protection are defined.

Keywords

networking, IoT, digital age, privacy, personal data protection, IoT challenges.

I. INTRODUCTION

Network space is the basis for the development of modern technologies in the digital age and determines the characteristics of communications between users. A large amount of information is distributed in the network space, including personal data. This is true for both the public and private sectors, where a very large proportion of information is collected, processed and stored in electronic form at some stage of its life cycle. This poses the important problem of ensuring the necessary level of computer security and data protection in the network space. The same is valid for IoT too.

The main goal of the article is to systematize specific features of the network space and IoT in particular, defining the main challenges to the privacy and protection of users' personal data. In this case, it is specified that many of the possible problems of the network space also reflect on those for IoT, and an example formulation of IoT security is given

II. Social Aspects of Internet Space

A. Social communications in the network space

Communications are directly related to human activity and are inherent in the mental characteristics of human associations. . In a modern aspect, the term "communication" is associated with means of connection with objects of the material and spiritual world, as well as communication and exchange of information in society and in private from person to person. This adds to the term the adjective "social", which is associated with social life, social class, social contacts, and social clubs. In a modern aspect, social communications are directly related to the network space.

B. Functional relations "user-device"

Electronic devices that are used for communications in the network space expand their functional capabilities beyond the performance of only specific service commitments for the exchange of information. This raises the question of people's relationship with electronic devices (e-devices), which they use for work, learning, contacts, obtaining information, gathering data, entertainment, etc. The result is a change in the human-human relationship to a new type of human-device.

The e-devices themselves are in certain interrelationships with each other in terms of the way of use and the specifics of the services they provide. Their functions are complemented by various mobile, portable, or stationary devices that are used where people are most often – at home, office, car or in public places. This determine some challenges for personal data protection and user privacy.

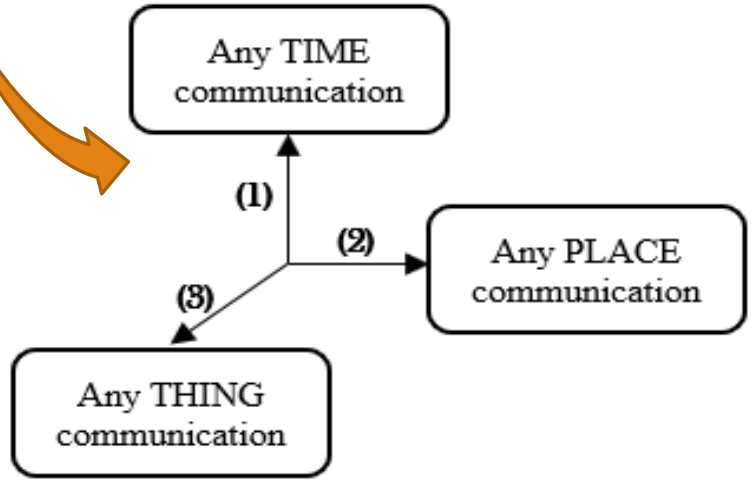
III. Features of Internet of Things

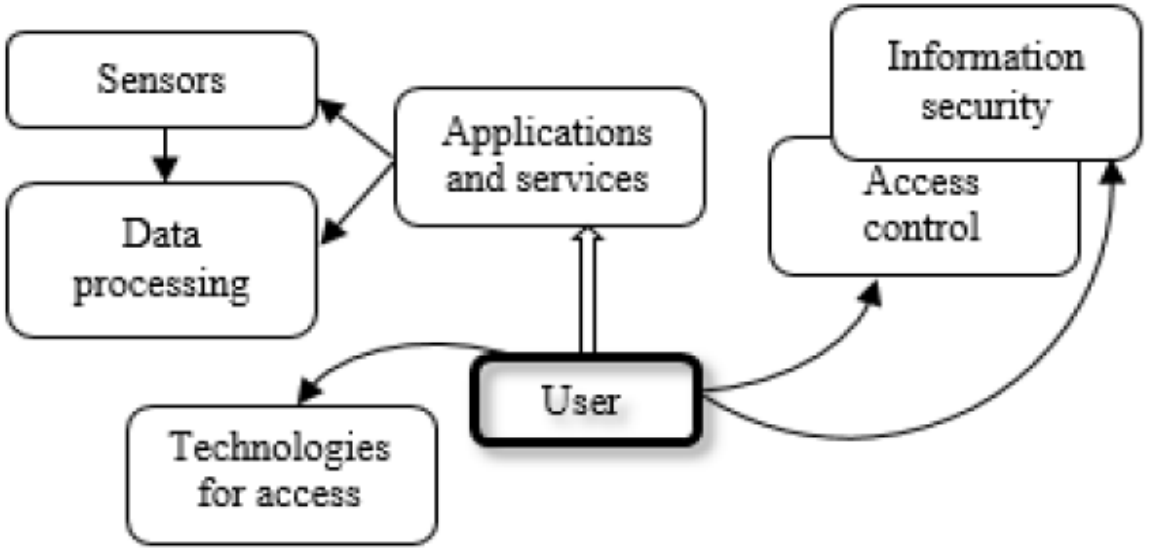
1. Short history aspects of IoT creation and development is presented. According to the definition of the International Telecommunication Union (ITU), it is a global infrastructure for the provision of complex services based on the connection through ICT of different things that can send and receive data.

2. IoT add a new dimension to the communications

3. Two types of thing can be determined: ✓ Physical things that exist in the physical world and can be measured, activated, and connected; .✓ Virtual things that exist in the information world and can be stored, processed, and accessed.

4. Formal description of possible functional communications and relations between IoT components is presented in Figure below





IV. Problems for Privacy in IoT

A. Data protection in the network space

User privacy in the Internet space is an important problem which is an object of discussion and regulation. The main requirement is that the information published in the websites must be correct, reliable and that the necessary protection measures have been taken. This is the responsibility of the site owner (Data Controller), who must ensure the necessary protection of personal data for the Data Subject.

The service provider must comply with the following rules.

✓ Confidential communication – prohibition of listening, interception, or storage of messages without the consent of the Data Subject.

✓ Ensuring the reliability and security of the services provided through appropriate security measures.

✓ Timely notification of the Data Subject and the national authority in the event of an open violation of his personal data.

✓ Confidentiality of subscriber traffic and location data, data can be deleted or anonymized.

✓ Explicitly requiring user consent before sending unsolicited messages (spam).

✓ Giving prior consent to the Data Subject to include data (phone number, address, email, etc.) in public directories.

✓ Restrictions on caller identification through the option, if desired, to not display the caller's personal phone number when connecting.

B. IoT security and user privacy

IoT security = [net]+[app]+[mobile]+[cloud]

Component	*Security*
Network [net]	Services, Protocol, Encryption, Firewall, Input, Providers, Third party access point, etc.
Applications [app]	Authentication, Authorization, Input validation, Web-based attack, etc.
Mobile [mobile]	Rooted device, Malware app, Insecure APIs. Lack of encryption, etc.
Cloud [cloud]	Session-based Authentication, Service provider, etc.

Some considerations regarding privacy protection in IoT are summarized below.

✓ IoT privacy is one of the specific considerations for providing reliable personal data protection because almost any physical or logical object or object can be given a unique identifier and the ability to communicate freely over the Internet or other network.

✓ IoT security is also an issue because the multitude of Internet devices and computers involved are often configured with standard or weak passwords, are not reliably secured, and things can be used as separate attack targets.

✓ There is a lack of incentives to build cybersecurity and privacy into IoT devices, paying more attention to market characteristics (price, priorities, etc.).

✓ The growth of IoT devices leads to a significant accumulation of data, which can lead to certain security and privacy risks.

✓ The various devices used in the organization of IoT are usually the subject of different manufacturers, which does not guarantee the construction of a common "cyber-hygiene".

V. Conclusion

Each of the modern technologies (Social Communications, Cloud Computing, Internet of Things, Big Data Analytics, etc.) creates new challenges to personal privacy due to the specifics of the processes and in particular the treatment of the concept of "personal data" in cross-border transfers.

The main challenges can be briefly systematized as breaches in the security of systems, misuse of data collected for other purposes, collection of data outside the jurisdiction of the Data Controller, invalidation of the principle of "minimization of personal data collected", violation of processing transparency and anonymity of the data, as well as the possibility that subsequent analysis for decision-making may lead to a violation of the privacy of the participants. All this requires an adequate evaluation of the processes and taking strict measures to protect the privacy of users.

REFERENCES

14 publications are included in the list of references

Thank you for your attention

Radi Romansky, rrom@tu-sofia.bg