Intelligent information systems

UDC 004.94 doi: 10.20998/2522-9052.2017.1.06

A. Goriushkina[1], R. Korolev[2]

[1] National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
[2] Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine

ANALYSIS OF THE CURRENT STATUS OF INTELLIGENT SYSTEM "INTERNET OF THINGS" AND TRENDS IN THE DEVELOPMENT

The **subject** of study in the article is the processes of analysis and evaluation of attack intelligent systems “Internet of Things” (IoT). The goal is to reduce the potential attacks due to the risks of intellectual functioning of the IoT systems, through the timely adoption of security measures. **Objectives:** the classification of attacks on all levels of intelligent systems, IoT, highlighting the main factors and their causes; the following results are obtained. The analysis of the current state of intelligent systems, IoT, analyzed all levels of functioning, and classification of hackers on the factors of their occurrence. The negative consequences negatively affecting the basic characteristics of the functioning of the IoT systems. As a result, a block diagram of attacks at all levels of the IoT. **Conclusions.** The article analyzes the current state of intelligent systems “Internet of Things” (IoT). It is shown that a significant increase in computer network devices connected to the network creates new opportunities for the development of modern society in the field of science and technology. However, the significant development of “Internet of Things” is directly proportional to increases the possibility of attacks in computer networks. Therefore, the scientific direction improvement of existing or development of new algorithms, models, and their implementation to ensure major safety criteria for IoT are relevant.

Keywords: intelligent systems Internet of Things, attacks, security, computer technology.

Introduction

The rapid development of modern society and computer technology offers consumers a wide range of services. To date, the significant growth of networked network devices, systems and services included in the current structure, create new opportunities and advantages for the development of modern society in science, technology and industry.

The devices connected to the Internet allow for high-level communication between users, the network and various types of provided physical services. Such connections are highly effective, and they also open the possibility of using new ways of using the Internet resource. Cloud computing can provide the virtual infrastructure for such utility computing which integrates monitoring devices, storage devices, analytics tools, visualization platforms and client delivery. The cost based model that cloud computing offers will enable end-to-end service provisioning for businesses and users to access applications on demand from anywhere. Smart connectivity with existing networks and context-aware computation using network resources is an indispensable part of Internet of Things.

The analysis of the problem and formulation of the task

“Internet of Things” (IOT) is a global network infrastructure, linking physical and virtual object s through the exploitation of data capture and communication capabilities. It will offer specific object identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterized by a high degree of autonomous data capture, event transfer, network connectivity and interoperability.

As recent studies have shown the popularity of different paradigms varies with time. Analysis of trends in the development of the demand for computer resources by users is shown in Fig. 1. As it can be seen, since IoT has come into existence, search volume is consistently increasing with the falling trend for others.

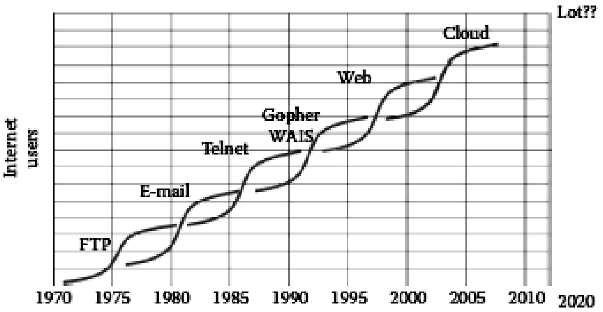


Fig. 1. Analysis of trends in the development of the demand for computer resources by users

In this case, it is shown a schematic of the interconnection of objects is depicted in Fig. 2, where the application domains are chosen based on the scale of the impact of the data generated.

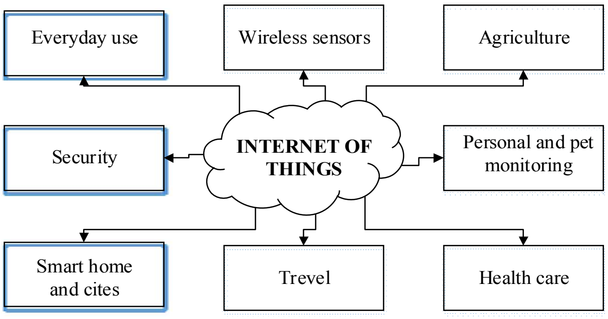


Fig. 2. IoT schematic of end users and application areas based on data

The users span from individual national level organizations addressing wide ranging issues.

According to the research conducted, in connection with the rapidly growing technology Internet of things, over the past 10 years, the tendency of attacks from hackers to different levels of the Internet of Things architecture has significantly increased.

The Fig. 3 shows the statistics of attacks on the Statistics of attacks of the IoT.

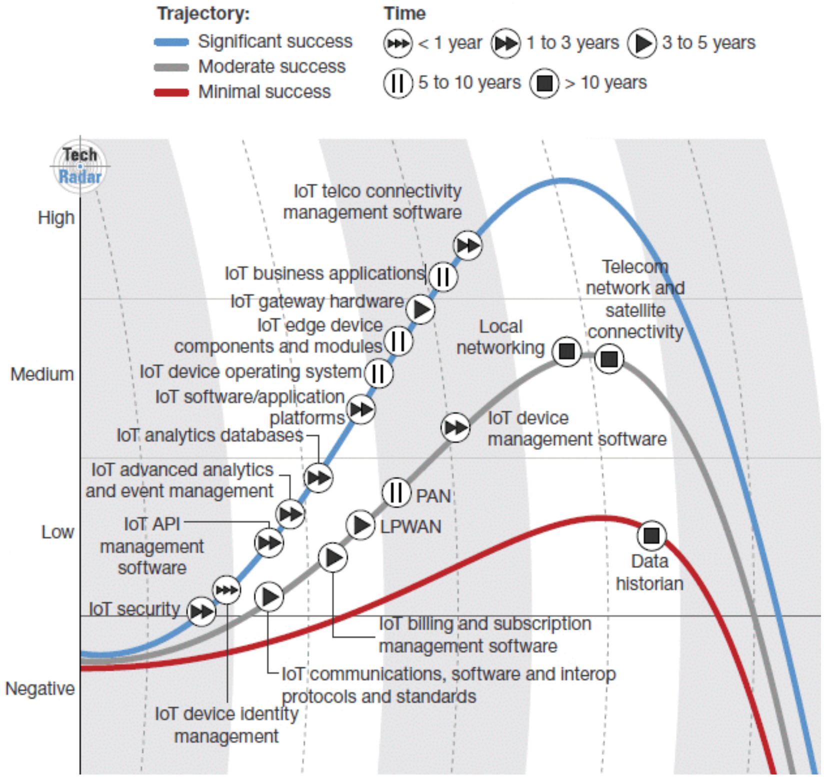
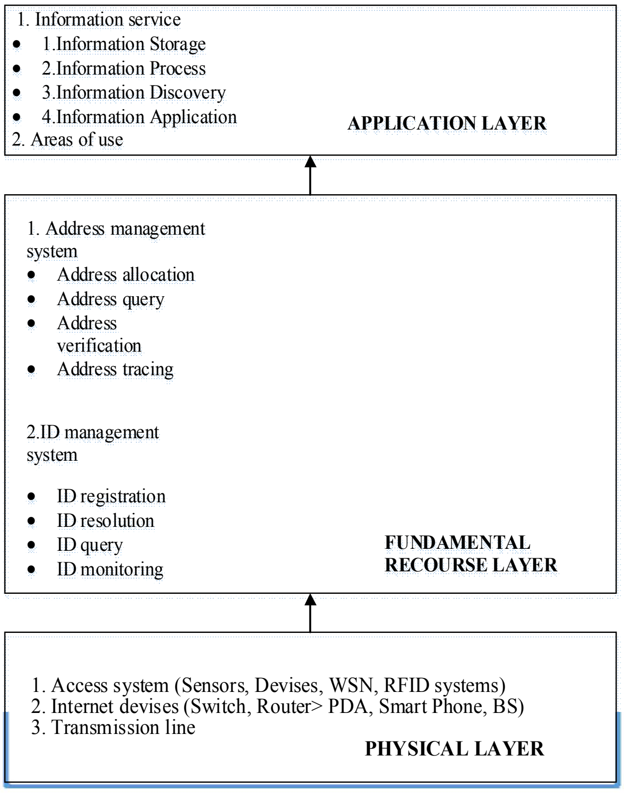


Fig. 3. Statistics of attacks of the IoT

Task solution

IoT combines end-user systems, data centers, digital devices, RFID, sensors and chips, intelligent devices and networks, cloud computing, vehicle networks, and other storage media. These results in the generation of enormous amounts of data which have to be stored processed and presented in a seamless, efficient, and easily interpretable form.

The main levels of IOT architecture are these 3: the perception level, the network level, and the service level, as shown in Fig. 4.



1. Information service
- 1.Information Storage
- 2.Information Process
- 3.Information Discovery
- 4.Information Application

2. Areas of use

APPLICATION LAYER

1. Address management system
- Address allocation
- Address query
- Address verification
- Address tracing

2.ID management system
- ID registration
- ID resolution
- ID query
- ID monitoring

FUNDAMENTAL RECOURSE LAYER

1. Access system (Sensors, Devises, WSN, RFID systems)
2. Internet devises (Switch, Router> PDA, Smart Phone, BS)
3. Transmission line

PHYSICAL LAYER

Fig. 4. Internet of Things system architecture

Physical layer. On this level all kinds of information of the physical world used in IOT are perceived and collected in this level, by the technologies of sensors, wireless sensors network (WSN),tags intelligent terminals, electronic data interface (EDI), objects, and so on.

The second layer is Fundamental recourse layer. It consist network level or transport layer and support layer. It’s including access network and core network, provides transparent data transmission capability. At the same time, this layer provides an efficient, reliable, trusted network infrastructure platform to upper level and large scale industry application.

Application layer includes data management sub-layer and application service sub-layer. The application service sub-layer transforms information to content and provides good user interface for upper level enterprise application and end users.

There are three IoT components which enables seamless connection:

Hardware—made up of sensors, actuators and embedded communication hardware.

Middleware—on demand storage and computing tools for data analytics.

Presentation—novel easy to understand visualization and interpretation tools which can be widely accessed on different platforms and which can be designed for different applications.

IoT affects the functioning of elements of a heterogeneous structure with a great distance of the control centers from each other. In this regard, the importance of ensuring the quality of service when transferring data in computer networks. It is also obvious that the process of information exchange of IoT data is complicated from the point of view of interaction of various protocols, and its functionality in general.

As studies [1-8] show, an increase in the demand growth by users for these resources in computer networks leads to some undesirable consequences, namely, various attacks on this system, in which existing methods and protection algorithms are not able to ensure the required level of security.

The security of information and network should be equipped with these properties such as identification, confidentiality, integrality and accessibility. Network security and management play an important role in above each level, which was considered.

The analysis showed common security requirements for each level, as shown in Fig. 5.

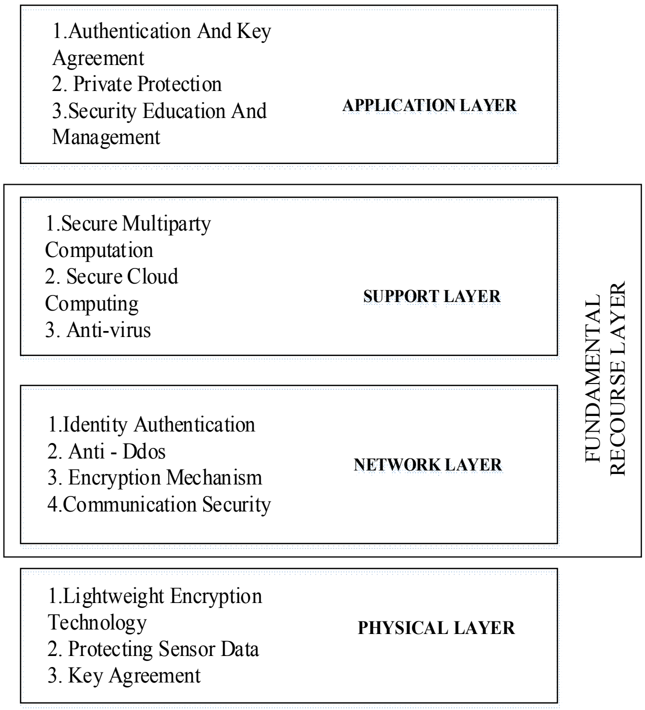

1.Authentication And Key Agreement
2. Private Protection
3.Security Education And Management
APPLICATION LAYER
1.Secure Multiparty Computation
2. Secure Cloud Computing
3. Anti-virus
SUPPORT LAYER
1.Identity Authentication
2. Anti - Ddos
3. Encryption Mechanism
4.Communication Security
NETWORK LAYER
FUNDAMENTAL RECOURSE LAYER
1.Lightweight Encryption Technology
2. Protecting Sensor Data
3. Key Agreement
PHYSICAL LAYER

Fig. 5. Security requirements of IoT

Analysis of the literature [1-8] showed that with the increase in the number of interacting IoT objects, the likelihood of attacks in the computer network is also growing proportionally.

For the qualitative work of the intelligent IoT system, it is necessary to carry out a sequence of actions, consisting of five steps, from receiving the initial data to the final delivery of this data to end users. At the same time, at each stage there is a possibility of a threat of attack from hackers.

Let's consider different types of attacks on Internet of Things systems on the example of data transfer in these systems as shown in Fig. 6.

Conclusions

In the last few years, this emerging domain for the IoT has been attracting the significant interest, and will continue for the years to come. In spite of rapid evolution, we are still facing new difficulties and severe challenges. The significant growth of threats and attacks in the field of computer systems and IoT facilities leads to an increase in the measures taken to ensure an appropriate level of security. First of all, effective mechanisms are considered that can identify the attack resistance necessary for the high-quality operation of the IoT intelligent network.

In this article, we consider the at- maturity of research into intelligent systems. The main levels of architecture and security issues at each level are considered. An example of data transmission in the intellectual Internet of things is shown, and atk types of attacks during data transmission. Obviously, under similar circumstances, the issue of the security of intelligent systems is relevant. Therefore, the actual directions are the improvement of existing or development of new algorithms, models and their implementation to provide basic IoT security criteria such as identification, confidentiality, integrity and accessibility.

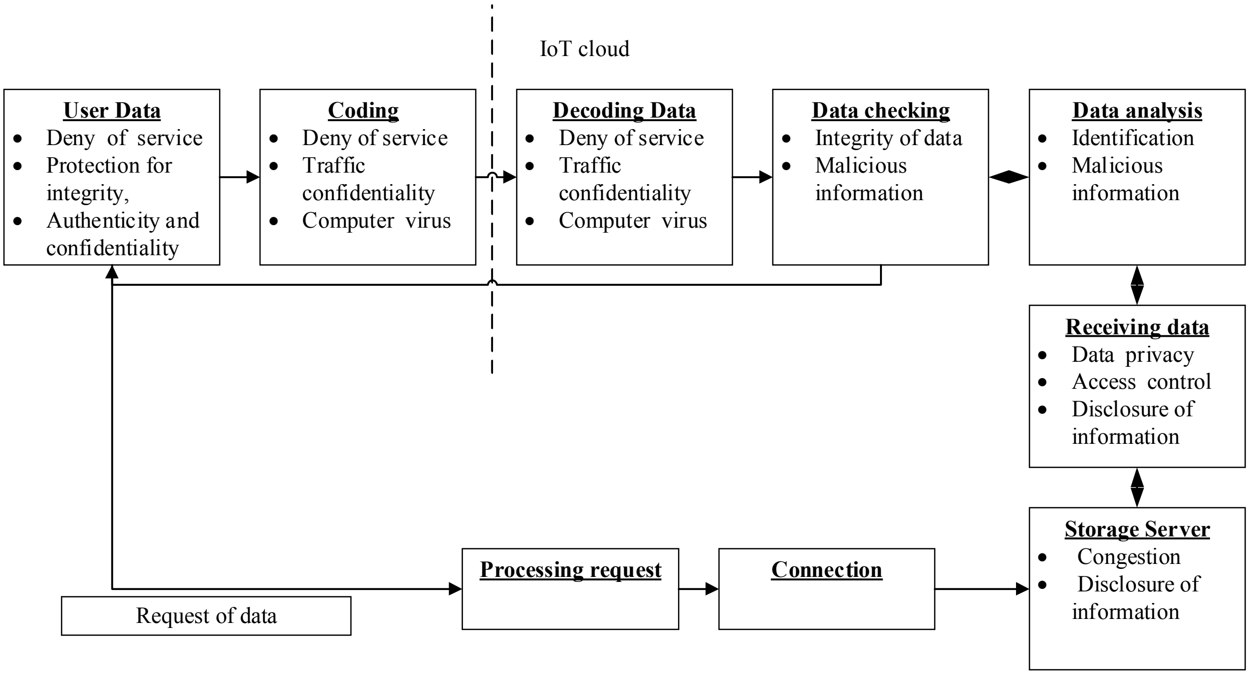


Fig. 6. Different types of data transfer attacks on Internet of Things systems

REFERENCES

1. Chuankun, Wu. (2010), "A preliminary investigation on the security architecture of the Internetof Things", *Strategy and Policy Decision Research*, 25(4), pp. 411–419.
2. Goldman, Sachs (2014), IoT Primer, The Internet of Things: Making Sense of the Next Mega-Trend, September 3, available at : http://www.goldmansachs.com/our-thinking/outlook/internet-of-things/iot-report.pdf (last accessed March 23, 2017).
3. International Telecommunication Union. ITU Internet reports 2005: The Internet of Things (2005), 212 p.
4. Ibrahim, Mashal, Osama, Alsaryrah, Tein-Yaw, Chung, Cheng-Zen, Yang, Wen-Hsing, Kuo and Dharma, P. Agrawal (2015), "Choices for interaction with things on internet and underlying issues", *Ad Hoc Networks*, 28, pp. 68–90.
5. Jeyanthi ang N.,N.Ch.S.N. Iyengar. (2013), "Escape-on-sight: An efficient and scalable mechanism for escaping DDoS attacks in cloud computing environment", *Cybernetics and Information Technologies*, 13(1), pp. 46–60.
6. Kang, Kai, Pang, Zhibo and Wang Cong (2013), "Security and privacy mechanism for health Internet of Things", *The Journal of China Universities of Posts and Telecommunications*, 20 (Suppl. 2), pp. 64–68.
7. Kim Thuat Nguyen, Maryline Laurent and Nouha Oualha (2015), "Survey on secure communication protocols for the Internet of Things", *Ad Hoc Networks*, 32, pp. 17–31.
8. Qazi Mamoon Ashraf ang Mohamed Hadi Habaebi (2015), "Autonomic schemes for threat mitigation in Internet of Things", *Journal of Network and Computer Applications*, 49, pp. 112–127.
9. Jia, X.L., Feng, Q.Y. and Ma, C.Z. (2010) "An efficient anti-collision protocol for RFID tag identification", *IEEE Communications Letters*, vol. 14, no. 11, pp.1014–1016.
10. Finkenzeller K. (2010), RFID *Handbook: Fundamentals and Applications in Contactless Smart Cards*, Radio Frequency Identification and Near-Field Communication, New York: Wiley. – 478 p.
11. Culler D {2003), "10 Emerging Technologies That Will Change the World", *Technology Review*, pp. 33–49.
12. Lu, Y.X., Chen, T.B., Meng, Y. (2011), "Evalution guideling system and intelligent evaluation process on the Internet of Things," *American Journal of Engineering and Technology Research*, vol. 11, no.9, pp.537-541.
13. Bang O., Choi J.H., Lee D. and Lee H. (2009), *Efficient Novel Anti-collision Protocols for Passive RFID Tags*, Auto-ID Labs White Paper WP-HARDWARE-050, MIT, 29 p.

Надійшла (received) 03.04.2017
Прийнята до друку (accepted for publication) 13.06.2017

Аналіз сучасного стану інтелектуальної системи "Internet of Things" та тенденції її розвитку

А. Е. Горюшкіна, Р. В. Корольов

Предметом вивчення в статті є процеси аналізу та оцінки атак інтелектуальної системи "Internet of Things" (IoT). **Мета** – зниження потенційних атак, зумовлених ризиками функціонування інтелектуальної системи IoT, шляхом своєчасного вжиття заходів безпеки. **Завдання:** класифікація атак на всіх рівнях інтелектуальної системи IoT з виділенням основних факторів і причин їх виникнення; Отримані наступні **результати**. Проведено аналіз сучасного стану інтелектуальної системи IoT, проаналізовано всі рівні функціонування та класифікацію атак хакерів за факторами їх виникнення. Визначено негативні наслідки, що негативно впливають на основні характеристики функціонування IoT. В результаті сформована структурна схема атак на всіх рівнях IoT. **Висновки.** У статті аналізується поточний стан інтелектуальної системи "Internet of Things." Показано, що значне зростання комп'ютерних мережевих пристроїв, підключених до мережі створює нові можливості для розвитку сучасного суспільства в галузі науки і техніки. Однак, значний розвиток "Internet of Things" прямо пропорційно збільшує можливість атак в комп'ютерній мережі. Тому наукові напрямки вдосконалення існуючих або розробка нових алгоритмів, моделей та їх реалізації для забезпечення основних критеріїв безпеки для IoT є актуальними.

Ключові слова: інтелектуальна система "Internet of Things", атаки, безпека, комп'ютерні технології.

Анализ современного состояния интеллектуальной системы "Internet of Things" и тенденции ее развития

А. Э. Горюшкина, Р. В. Королев

Предметом изучения в статье являются процессы анализа и оценки атак интеллектуальной системы "Internet of Things" (IoT). **Цель** – снижение потенциальных атак, обусловленных рисками функционирования интеллектуальной системы IoT, путем своевременного принятия мер безопасности. **Задачи**: классификация атак на всех уровнях интеллектуальной системы IoT с выделением основных факторов и причин их возникновения; Получены следующие результаты. Проведен анализ современного состояния интеллектуальной системы IoT, проанализированы все уровни функционирования и классификацию атак хакеров по факторам их возникновения. Определены негативные последствия, негативно влияющие на основные характеристики функционирования IoT. В результате сформирована структурная схема атак на всех уровнях IoT. **Выводы.** В статье анализируется текущее состояние интеллектуальной системы "Internet of Things". Показано, что значительный рост компьютерных сетевых устройств, подключенных к сети, создает новые возможности для развития современного общества в области науки и техники. Однако, значительное развитие "Internet of Things" прямо пропорционально увеличивает возможность атак в компьютерной сети. Поэтому, научные направления совершенствования существующих или разработка новых алгоритмов, моделей и их реализации для обеспечения основных критериев безопасности для IoT являются актуальными.

Ключевые слова: интеллектуальная система "Internet of Things", атаки, безопасность, компьютерные технологии.