IRSTI 81.93.29

A. Adamova[1], T. Zhukabayeva[1], Khu Ven-Tsen[2]

[1]Astana IT University, Astana, Kazakhstan
[2]M. Auezov South Kazakhstan State University, Shymkent, Kazakhstan
*E-mail: *Aigul.adamova@astanait.edu.kz*

Internet of Things: Security and Privacy standards

Abstract. *Ensuring security in the interaction of the Internet of Things (IoT) has focused the attention of many researchers. At present, the issue of standards is a very complex and important one that directly affects both the development and implementation of the Internet of Things in everyday life. There are many standards and protocols that may not be consistent across different layers of the architecture. This paper provides an overview of the current International Internet of Things Security Standards, which are discussed in various aspects such as terminology, architecture models, security and integration scenarios, classification and protocols. A comparative analysis of standards and related research is conducted to help inform decisions about the security of IoT systems during their development and production. This research aims to overcome the difficulties encountered and develop practical recommendations for the selection of controls and security of connected IoT devices. The research methodology included identification of gaps in IoT standards, analysis of existing problems and proposed solutions.*
Keywords: *Internet of Things, security, communication, standard, attack.*

DOI: doi.org/10.32523/2616-7263-2023-144-3-29-40

Introduction

Modern achievements of scientific and technological progress in the field of information technology and communications have led to the emergence and explosive development of a qualitatively new type of information and communication networks, called the Internet of Things (IoT). IoT is a network of actively interacting physical objects and technologies, in which the exchange of information between connected devices and systems is provided through the Internet [1].

IoT is the basis and driving force for a wide range of smart applications that have been developed at the level of facilities of various sizes – from smart home to smart city, smart industries and industry in general, education and healthcare, agro-industrial sector, etc. With each day, the number of connected objects and devices of the Internet of Things is constantly and rapidly increasing, in connection with the problems inherent in information and telecommunication networks, in particular, ensuring IoT security [2-4]. Measures were aimed at solving these problems, including the adoption of international standards for the unification of IoT systems, ensuring their interoperability and security.

The development and adoption by international organizations of various Internet security standards is an effective measure. However, with the abundance of these standards, determining the most appropriate in each specific case can be difficult. In this regard, it seems practically important and relevant to conduct a comprehensive comparative analysis of international IoT security standards to facilitate the adoption of appropriate decisions in their development and production.

Today, organizations such as ENISA, NIST and a number of others are successfully operating and have published security requirements for IoT products [3, 4]. Along with this, many countries (USA, Australia, Great Britain, Singapore, etc.) have developed and implemented regulatory documents that help reduce the risks from cyber-attacks.

In 2019, the European Telecommunications Standards Institute (ETSI) Technical Committee Cybersecurity (TC CYBER) published the first cybersecurity standard for consumer devices in the Internet of Things (ETSI TS 103 645) category.

In 2020, the ETSI TC CYBER released an update to the IoT security standard TS 103 645 – ETSI EN 303 645, "which establishes a security baseline for Internet-connected consumer products and provides a foundation for future IoT certification schemes." It is currently the most widely used standard in this area. Its role in Europe is to support European regulation and legislation through the development of harmonized European standards. It has 900 members from over 60 countries, many of which are outside the EU, such as Vietnam, Finland, Singapore.

In 2022 NIST published its *Baseline Security Criteria for Consumer IoT Devices*. 2022, the standard was developed based on the NIST white paper: *Recommended Criteria for Cybersecurity Labeling for IoT Consumer Products*. The work of ISO/IEC, an international non-governmental organization, is also relevant. Although less accepted at present, he has published a number of standards including ISO/IEC 27402.

In 2021, India introduced the standard *Code of Practice for Securing Consumer Internet of Things (IoT) (TEC 31318:2021)*, an approach based on ETSI TS 103 645 and EN 303 645. It is also expected that ETSI TS Standard 103 701 (Cybersecurity Assessment for Consumer IoT Products) will help in the implementation of these recommendations.

In 2020, the Ministry of Economy, Trade and Industry of Japan (METI) launched *IoT Security Safety Framework* (IoT-SSF).

In 2020, the South Korean Internet and Security Agency (KISA) released Guidelines on Automated Processing (Guidelines), Internet of things (IoT), and Privacy by Design.

In 2020, Russia developed national standards for the secure Internet of things. They were created by the Cyber-Physical Systems technical committee on the basis of RVC and Kaspersky Lab [5].

To ensure the security of IoT systems, it is necessary to take into account the compatibility and commonality of the applied standards. International standards ensure interoperability by listing protocols, rules, guidelines and characteristics that are defined and approved by authorized organizations. Interoperability and security are also supported by the adoption of standards in the development and management of IoT systems.

Methodology

The ongoing research was aimed at identifying gaps and problems in the current international IoT security standards. At the first and second stages, research papers were searched in the IEEE Xplore, Google Scholar, Science Direct databases using the keys "IoT Security Standard", "IoT Security Challenges" for 2022-2023. At the third stage, the search was carried out using double keys - "IoT Security" and "Open Problems" or "IoT Security" and "IoT Security Challenges". At the fourth stage, an analysis was made of the selection of works in the direction of the study. At the final fifth stage, works were selected that have open access for the analysis of the proposed solutions (Fig. 1).

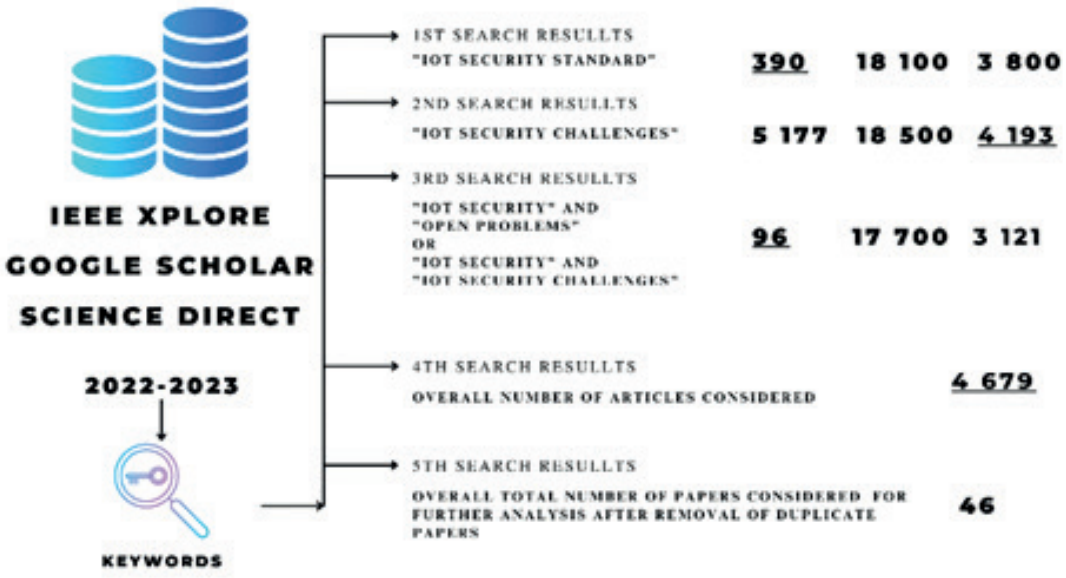


Figure 1. Research Methodology

IoT Device Security Scores by Country

With the rapid growth of IoT in various sectors, there is an increase in the number of recorded attacks in them. The above map shows the definition of countries by the number of attacks committed in 2022. Countries with the highest percentage of attacks are highlighted in red, countries with the lowest number of attacks are highlighted in green, countries with an average percentage are shown in yellow and blue. As it turned out, the number of attacks directly depends on the number of connected devices in IoT systems, low percentages do not guarantee better protection, and with an increase in the use of IoT devices, the indicators can increase dramatically (Fig. 2).

According to SOURCE, the TOP countries with the lowest rate of telnet attacks include Haiti, Tajikistan, Algeria, Qatar and Tajikistan for attacks based on SSH. With the highest rate of telnet attacks are – India, China, Egypt; for attacks based on SSH – China, United States.

Data presented in [6] show that Telnet vulnerabilities can be exploited by attackers and provide access to IoT devices, allowing you to change devices and monitor any data transmitted. SSH is used for remote login, command execution, file transfer, and more. SSH brute force attacks are often achieved by having the attacker try a common username and password on thousands of servers until they find a match. [7].

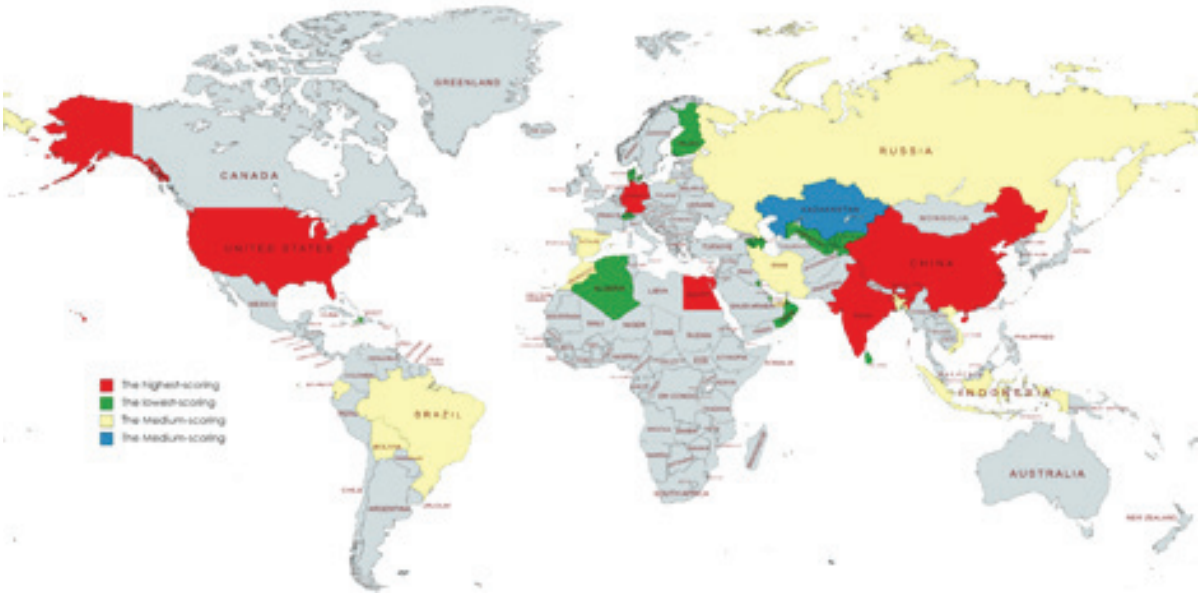


Figure 2. TOP countries with the lowest/highest rate

Description of standards

Standards are mainly formed in the following categories:

- definitions of basic IoT security terms introduces the concept of basic security of IoT devices and unifies the understanding and use of terms in the direction;
- architecture models – consideration of various IoT architectures, and definition of functions, relationships, communication with the cloud, etc.;
- security scenarios – consideration of various types of scenarios, provision of IoT security requirements;
- security integration – security at all levels of the infrastructure, through the planning and implementation of IoT;
- security classification – basic principles, measurements, IoT security methods and basic support for the implementation of hierarchical control;
- security protocols – consideration between the IoT platform, the gateway, the terminal itself and the equipment, including wired protocol security, wireless protocol security, storage protocol security, etc.

IoT devices are defined by having an embedded operating system that does not support the installation of security agents such as antivirus and is not suitable for frequent software updates. The standards apply to all IoT devices connected to the network [8, 9]. Table 1 lists the names of international standards with an example and description.

Table 1. Standards of IoT security

Standard	Description	Data
ISO/IEC	related to information technology, security techniques, privacy, incidence response, risk management (total 80 standards)	
ISO/IEC 27400:2022	guidelines on risks, principles and controls for security and privacy of IoT solutions	2022-06
ETSI	focus on Smart cities, Smart Grids, Smart Metering, Smart Body Area Networks, Smart Cards, Different area of cybersecurity, Different area of IoT (total 32 standards)	
ETSI GS MEC 033 V3.1.1 (2022-12)	multiple Access Edge Computing (MEC); IoT API	2022-12
ETSI SR 003 680 V1.1. (2020-03)	smartM2M; Guidance on security, privacy and interoperabilit in defining an IoT system; Specific Approach	2020-03
ETSI TR 103 778 V1.1. (2021-12)	smartM2M; Use cases for cross-domain use of IoT device data	2021-12
NIST	guide to Software, IoT Security and Labeling	
NIST IR 8454	evaluation and standardization of lightweight cryptographic algorithms suitable for use in restricted environments	2023-02
NIST 800-82	industrial System Security	2015-05
IEEE	a method for data sharing, interoperability, and security of messages over a network, where sensors, actuators and other devices can interoperate, regardless of underlying communication technology.	
IEEE 2668-2022	IoT maturity index	2022-12
ANSI/ISA	focus on processes, techniques and requirements for industrial automation and control systems	
ANSI/ISA/IEC 62443	security for Industrial Automation and Control Systems	2018-02

In 2022, the UK Telecommunications Infrastructure Security Bill was passed which would require IoT device manufacturers to no longer use default passwords, confirm how long security updates will be provided after a device is launched, and disclose known vulnerabilities.

The EU has also taken steps to improve the security of all IoT devices sold in Europe, where security is not currently provided. The proposed European Cyber Resilience Act requires IoT devices to have "an appropriate level of cybersecurity enabled in devices" by default, prohibits the sale of products with known vulnerabilities, and requires minimizing the impact of security incidents. While the implementation of the necessary security controls is yet to be determined, these are critical initial steps to promote the adoption of widespread security controls for IoT devices in Europe.

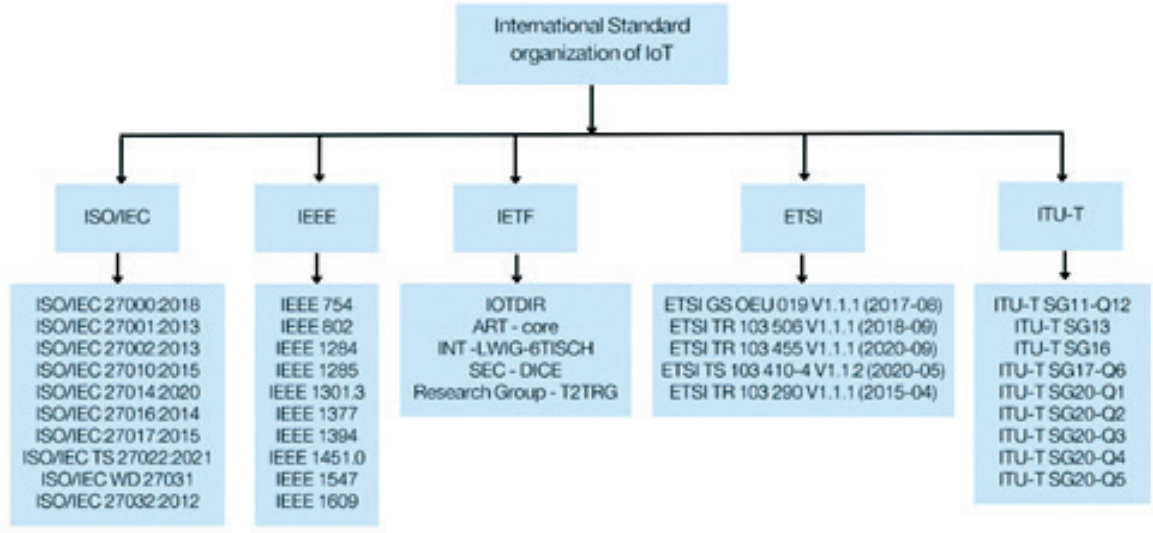
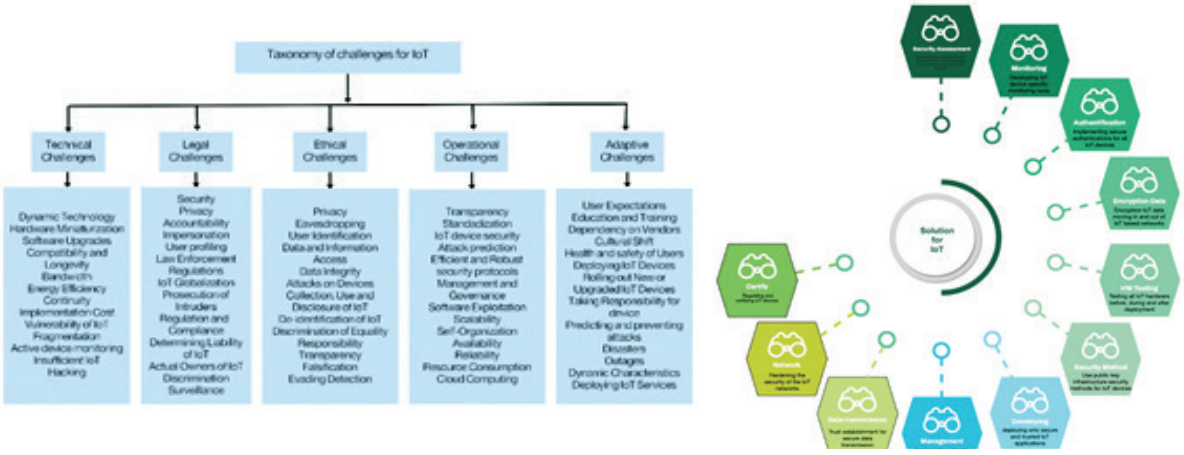


Figure 3.International Standard

Figure 4 shows suggested possible solutions that contribute to the security of systems deployed within the IoT.



(a) (b)

Figure 4. Taxonomy of Challenges (a) and Suggested solutions (b)

Review of Works

Table below provides an overview and analysis of published papers on the subject of the study.

Table 2. Review of Work

Work	Author	Year	Title	Source	Description
[10]	NM Karie, et al.	2021	A Review of Security Standards and Frameworks for IoT-Based Smart Environments	IEEE Access	The authors provide an overview of international security standards ISO/IEC, ETSI and various structures, including methods proposed by NIST. The authors note the need to develop standards for the security of IoT-based systems.
[11]	A. Khurshic et al.	2022	EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme	IEEE Access	The paper proposes a template for security certification of IoT devices as a result of the analysis of international requirements for certification. An evaluation of the proposed approach using the ENISA qualification system is given and compliance with the criteria of the EC certification scheme is demonstrated.
[12]	Qiu, Qin & Wang, et al.	2022	Security Standarc and Measures for Massive IoT in th 5G Era	Mobile Networks and Applications	The paper proposes standardization approaches that contribute to the successful development of IoT in 5G conditions.
[13]	Manju Lata, et al.	2021	Standards and Regulatory Compliances for IoT Security	International Journal of Service Science Management Engineering and Technology	The work is devoted to IoT security issues, the role of standards and regulatory requirements is highlighted.

[14]	Brass, Irina, et al.	2018	Standardizing Moving Targe The Developn and Evolutior of IoT Securit Standards.	Conference: Living in the Internet of Things: Cybersecurity of tl IoT - 2018	The paper describes the main standards, IoT security guidelines developed by various organizations profiling in the field of security. as a result, an approach is proposed for the development and implementation of standards.
[15]	Olga Greuter, et al.	2022	The baseline of global consumer cyber security standards for IoT: quality evaluation.	Journal of Cyber Security Technolog	the article assesses user standards for IoT security by comparing CSCIoT and IEC 6244.
[16]	Kaksonen, R., et al.	2022	Common Cybersecurity Requirements in IoT Standards, Best Practices, and Guidelines.	IoTBDS	The paper analyzes 16 sources, resulting in a set of general categories covering security design, interface security, authentication, data protection, and updates.
[17]	Svecova, H	2022	Design of a Method for Settin IoT Security Standards in Smart Cities.	Mobile Web and Intelligent Information Systems. MobiWIS 2022. Lecture Notes in Compute Science	The paper analyzes security standards and, as a result, proposes a method for complex processing of IoT security standards in smart cities.
[18]	Naraliyev, N., et al.	2019	Review and analysis of standards and protocols in the field of the Internet of Things. Modern testing methods and problems of information security IoT	International Journal of Open Information Technologies	The paper presents an overview of NIST, IEEE, ISO/IEC standards and other security solutions for IoT devices. along with this, various communication protocols and examples of building an ecosystem using IoT devices are considered.

[19]	Lee, E., et al	2021	A Survey on Standards for Interoperability and Security in th Internet of Things.	IEEE Communications Surveys & Tutorial	The paper presents an overview and analysis of standards developed by international organizations for IoT security. the problems of standards on interoperability and security of IoT devices are considered.

These works reflect the current state of IoT security standards, proposed tools, methodologies and security measures. They also cover the development and implementation of security standards for IoT devices and systems.

The above review of works can be divided into three thematic groups:

Review and analysis of IoT security standards and structures - [10, 12, 13, 14, 18, 19];

Proposal of IoT security standards and frameworks - [11, 17];

Evaluation of IoT security standards and frameworks - [15, 16].

Conclusion

With the proliferation of IoT devices and networks, it is critical to have robust standards and structures in place to secure them. The article presents a comparison from various perspectives of international security standards and related studies that can facilitate informed decision-making on the choice of the most appropriate security standard or framework for the projected or deployed Internet of Things, as well as in the production of its components. It is important to note that choosing an IoT security standard or framework is only the first step. Proper implementation and adherence to the chosen standard or framework is critical to ensure device reliability and IoT network performance.

In line with the goals and objectives set out in the "System of Standards", it is recommended to strengthen cooperation between industry, academia, research and applications. Pay attention to the combination and compatibility of the core security standards of the Internet of Things and the actual development of the industry, and promote the development of standards in a systematic manner. Implement dynamic updates. Specialists to monitor trends and trends in the development of new technologies and new applications of the Internet of things, actively adapt to the constant increase in the level of development of IoT security. Strengthen the dynamic update and improvement of the standard security system. To promote in every possible way the introduction of new standards and the deepening of their application.

Acknowledgments

This research is funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP14973006).

References

1. Lynn, T., Endo, P.T., Ribeiro, A.M.N.C., Barbosa, G.B.N., Rosati, P. (2020). The Internet of Things: Definitions, Key Concepts, and Reference Architectures. In: Lynn, T., Mooney, J., Lee, B., Endo, P. (eds) The Cloud-to-Thing Continuum. Palgrave Studies in Digital Business & Enabling Technologies. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-41110-7_1.
2. Statista 2023. https://www.statista.com (accessed: 01.06.2023)
3. ENISA https://www.enisa.europa.eu (accessed: 04.06.2023)
4. NIST https://www.nist.gov (accessed: 26.05.2023)

5. Kaspersky Laboratory http://www.kaspersky.ru (accessed: 01.06.2023)

6. Klein, James & Walcott, Kristen. (2020). Exploiting Telnet Security Flaws in the Internet of Things. 10.1007/978-3-030-12385-7_51.

7. Shrivastava, R.K., Bashir, B., Hota, C. (2019). Attack Detection and Forensics Using Honeypot in IoT Environment. In: Fahrnberger, G., Gopinathan, S., Parida, L. (eds) Distributed Computing and Internet Technology. ICDCIT 2019. Lecture Notes in Computer Science(), vol 11319. Springer, Cham. https://doi.org/10.1007/978-3-030-05366-6_33.

8. Nurlan, Z., Zhukabayeva, T., Othman, M., Adamova, A., & Zhakiyev, N. (2021). Wireless sensor network as a mesh: Vision and challenges. IEEE Access, 10, 46-67.

9. Nurlan, Z., Kokenovna, TZ, Othman, M., & Adamova, A. (2021). Resource allocation approach for optimal routing in IoT wireless mesh networks. IEEE Access, 9, 153926-153942.

10. N. M. Karie, N. M. Sahri, W. Yang, C. Valli and V. R. Kebande. A Review of Security Standards and Frameworks for IoT-Based Smart Environments. IEEE Access, vol. 9, pp. 121975-121995, 2021, doi: 10.1109/ACCESS.2021.3109886.

11. A. Khurshid, R. Alsaaidi, M. Aslam and S. Raz. EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme. IEEE Access, vol. 10, pp. 129932-129948, 2022, DOI: 10.1109/ACCESS.2022.3225973.

12. Qiu, Qin & Wang, Ding & Du, Xuetao& Yu, Shengquan& Liu, Shenglan& Zhao, Bei. Security Standards and Measures for Massive IoT in the 5G Era. Mobile Networks and Applications27. 10.1007/s11036-021-01841-2.

13. Manju Lata, Dr & Kumar, Vikas. Standards and Regulatory Compliances for IoT Security. International Journal of Service Science Management Engineering and Technology. 12. 133-147. 10.4018/IJSSMET.2021090109.

14. Brass, Irina &Tanczer, L. &Carr, Madeline & Elsden, M. & Blackstock, J. Standardising a Moving Target: The Development and Evolution of IoT Security Standards. Conference: Living in the Internet of Things: Cybersecurity of the IoT – 2018. 10.1049/cp.2018.0024.

15. Olga Greuter, K., &Sarmah, D. K. The baseline of global consumer cyber security standards for IoT: quality evaluation. Journal of Cyber Security Technology, 6(4), 175-200.

16. Kaksonen, R., Halunen, K., & Röning, J. Common Cybersecurity Requirements in IoT Standards, Best Practices, and Guidelines. IoTBDS (pp. 149-156).

17. Svecova, H. Design of a Method for Setting IoT Security Standards in Smart Cities. Mobile Web and Intelligent Information Systems. MobiWIS 2022. Lecture Notes in Computer Science, vol 13475. Springer, Cham. https://doi.org/10.1007/978-3-031-14391-5_9.

18. Naraliyev, N. A., & Samal, D. I. Review and analysis of standards and protocols in the field of Internet of Things. Modern testing methods and problems of information security IoT. International Journal of Open Information Technologies, 7(8), 94-104.

19. Lee, E., Seo, Y. D., Oh, S. R., & Kim, Y. G. A Survey on Standards for Interoperability and Security in the Internet of Things. IEEE Communications Surveys & Tutorials, 23(2), 1020-1047.

Интернет заттар: қауіпсіздік және құпиялылық стандарттары

А.Д. Адамова[1], Т.К. Жукабаева[1], Ху Вен-Цен[2]

[1]Astana IT University, Астана, Қазақстан

[2]М. Ауезов атындағы Оңтүстік Қазақстан Университеті, Шымкент, Қазақстан

Аңдатпа. Заттар интернеті (IoT) өзара әрекеттесу кезіндегі қауіпсіздікті қамтамасыз ету - көптеген зерттеушілердің назарын аударды. Қазіргі уақытта стандарттар мәселесі өте күрделі және маңызды, бұл заттар интернетін жасауға да, күнделікті өмірге енгізуге де тікелей әсер етеді. Бүгінгі күні көптеген стандарттар мен хаттамалар бар, олар архитектураның әртүрлі қабаттарында сәйкес келмеуі мүмкін. Ұсынылған мақалада терминология, архитектура модельдері, қауіпсіздік және интеграция сценарийлері, жіктеу және хаттамалар сияқты әртүрлі аспектілерде қарастырылатын қазіргі заманғы халықаралық заттар интернетінің қауіпсіздік стандарттарына шолу берілген. IoT жүйелерін әзірлеу және өндіру процесінде олардың қауіпсіздігін қамтамасыз ету бойынша негізделген шешімдер қабылдауға ықпал ететін стандарттар мен тиісті зерттеулерге салыстырмалы талдау жүргізілді. Бұл зерттеулер туындаған қиындықтарды жеңуге және қосылған IoT құрылғыларының қауіпсіздігін бақылау және қамтамасыз ету құралдарын таңдау бойынша практикалық ұсыныстар

жасауға бағытталған. Зерттеу әдістемесі IoT стандарттарындағы олқылықтарды анықтауды, бар мәселелер мен ұсынылған шешімдерді талдауды қамтыды.

Түйін сөздер: заттар интернеті, қауіпсіздік, коммуникация, стандарт, шабуыл.

Интернет вещей: стандарты безопасности и конфиденциальности

А.Д. Адамова[1], Т.К. Жукабаева[1], Ху Вен-Цен[2]
[1]Astana IT University, Астана, Казахстан
[2]Южно-Казахстанский государственный университет им. М. Ауезова, Шымкент, Казахстан

Аннотация. Обеспечение безопасности при взаимодействии интернет вещей сфокусировало внимание многих исследователей. В настоящее время вопрос по стандартам является очень сложным и важным, который напрямую влияет как на разработку, так и на внедрение интернет вещей в повседневную жизнь. Существует множество стандартов и протоколов, которые могут быть несогласованными в разных слоях архитектуры. В представленной статье приведен обзор современных международных стандартов безопасности интернета вещей (IoT), которые рассматриваются в различных аспектах, таких, как терминология, модели архитектуры, сценарии безопасности и интеграции, классификация и протоколы. Проведен сравнительный анализ стандартов и соответствующих исследований, которые способствуют принятию обоснованных решений по обеспечению безопасности систем IoT в процессе их разработки и производства. Эти исследования направлены на преодоление возникающих трудностей и разработку практических рекомендаций по выбору средств контроля и обеспечения безопасности подключенных IoT-устройств. Методология исследования включала выявление пробелов в стандартах IoT, анализ существующих проблем и предлагаемых решений.

Ключевые слова: интернет вещей, безопасность, коммуникация, стандарт, атака.

References

1. Lynn, T., Endo, P.T., Ribeiro, A.M.N.C., Barbosa, G.B.N., Rosati, P. (2020). The Internet of Things: Definitions, Key Concepts, and Reference Architectures. In: Lynn, T., Mooney, J., Lee, B., Endo, P. (eds) The Cloud-to-Thing Continuum. Palgrave Studies in Digital Business & Enabling Technologies. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-41110-7_1.
2. Statista 2023. https://www.statista.com (accessed: 01.06.2023)
3. ENISA https://www.enisa.europa.eu (accessed: 04.06.2023)
4. NIST https://www.nist.gov (accessed: 26.05.2023)
5. Kaspersky Laboratory http://www.kaspersky.ru (accessed: 01.06.2023)
6. Klein, James & Walcott, Kristen. (2020). Exploiting Telnet Security Flaws in the Internet of Things. 10.1007/978-3-030-12385-7_51.
7. Shrivastava, R.K., Bashir, B., Hota, C. (2019). Attack Detection and Forensics Using Honeypot in IoT Environment. In: Fahrnberger, G., Gopinathan, S., Parida, L. (eds) Distributed Computing and Internet Technology. ICDCIT 2019. Lecture Notes in Computer Science(), vol 11319. Springer, Cham. https://doi.org/10.1007/978-3-030-05366-6_33.
8. Nurlan, Z., Zhukabayeva, T., Othman, M., Adamova, A., & Zhakiyev, N. (2021). Wireless sensor network as a mesh: Vision and challenges. IEEE Access, 10, 46-67.
9. Nurlan, Z., Kokenovna, TZ, Othman, M., & Adamova, A. (2021). Resource allocation approach for optimal routing in IoT wireless mesh networks. IEEE Access, 9, 153926-153942.
10. N. M. Karie, N. M. Sahri, W. Yang, C. Valli and V. R. Kebande. A Review of Security Standards and Frameworks for IoT-Based Smart Environments. IEEE Access, vol. 9, pp. 121975-121995, 2021, doi: 10.1109/ACCESS.2021.3109886.
11. A. Khurshid, R. Alsaaidi, M. Aslam and S. Raz. EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme. IEEE Access, vol. 10, pp. 129932-129948, 2022, doi: 10.1109/ACCESS.2022.3225973.
12. Qiu, Qin & Wang, Ding & Du, Xuetao& Yu, Shengquan& Liu, Shenglan& Zhao, Bei. Security Standards and Measures for Massive IoT in the 5G Era. Mobile Networks and Applications27. 10.1007/s11036-021-01841-2.

13. Manju Lata, Dr & Kumar, Vikas. Standards and Regulatory Compliances for IoT Security. International Journal of Service Science Management Engineering and Technology. 12. 133-147. 10.4018/IJSSMET.2021090109.

14. Brass, Irina &Tanczer, L. &Carr, Madeline & Elsden, M. & Blackstock, J. Standardising a Moving Target: The Development and Evolution of IoT Security Standards. Conference: Living in the Internet of Things: Cybersecurity of the IoT – 2018. 10.1049/cp.2018.0024.

15. Olga Greuter, K., &Sarmah, D. K. The baseline of global consumer cyber security standards for IoT: quality evaluation. Journal of Cyber Security Technology, 6(4), 175-200.

16. Kaksonen, R., Halunen, K., &Röning, J. Common Cybersecurity Requirements in IoT Standards, Best Practices, and Guidelines. IoTBDS (pp. 149-156).

17. Svecova, H. Design of a Method for Setting IoT Security Standards in Smart Cities. Mobile Web and Intelligent Information Systems. MobiWIS 2022. Lecture Notes in Computer Science, vol 13475. Springer, Cham. https://doi.org/10.1007/978-3-031-14391-5_9.

18. Naraliyev, N. A., & Samal, D. I. Review and analysis of standards and protocols in the field of Internet of Things. Modern testing methods and problems of information security IoT. International Journal of Open Information Technologies, 7(8), 94-104.

19. Lee, E., Seo, Y. D., Oh, S. R., & Kim, Y. G. A Survey on Standards for Interoperability and Security in the Internet of Things. IEEE Communications Surveys & Tutorials, 23(2), 1020-1047.

Information about author:

A. Adamova – PhD, Assistant Professor, Astana IT University, 55/11 Mangilik El Ave., Astana, Kazakhstan.

T. Zhukabayeva – PhD, Professor, Astana IT University, 55/11 Mangilik El Ave., Astana, Kazakhstan.

Khu Ven-Tsen – Doctor of Technical Sciences, Professor, M. Auezov South Kazakhstan State University, 5 Tauke khan Ave., Shymkent, Kazakhstan.

А.Д. Адамова – PhD, профессор ассистенті, Astana IT University, Мәнгілік Ел даң., 55/11, Астана, Қазақстан.

Т.К. Жукабаева – PhD, қауымдастырылған профессор, Astana IT University, Мәнгілік Ел даң., 55/11, Астана, Қазақстан.

Ху Вен - Цен – т.ғ.д., профессор, М. Ауезов атындағы Оңтүстік Қазақстан Университеті, Тәуке хан даң., 5, Шымкент, Қазақстан.

А.Д. Адамова – PhD, ассистент профессора, Astana IT University, пр. Мәңгілік Ел, 55/11, Астана, Казахстан.

Т.К. Жукабаева – PhD, ассоциированный профессор, Astana IT University, пр. Мәңгілік Ел, 55/11, Астана, Казахстан.

Ху Вен-Цен – д.т.н., профессор, Южно-Казахстанский государственный университет им. М.Ауезова, пр. Тауке хана, 5, Шымкент, Казахстан.