Ontology-based model for security management in IoT systems*

Oleksiy Kovalenko[1,†] and Natalia Karevina[2,*,†]

[1] National University of Life and Environmental Sciences of Ukraine, 15 Heroyiv Oborony str., 03041 Kyiv, Ukraine
[2] Institute of Mathematical Machines and Systems Problems NAS of Ukraine, 42 Academic Hlushkov ave., 03187 Kyiv, Ukraine

Abstract

The development and implementation of Internet of Things (IoT) systems in modern conditions determines the special importance of addressing security issues and the sustainable functioning of such systems. The convergence of various technologies in IoT systems necessitates the collection, systematization and use of information on these technologies in problem-oriented knowledge bases for further use in security management processes in IoT systems. The use of an "ontological approach" provides conceptual connections between information assets of the system for identification, analysis and security management in systems. The implementation of the ontological approach is carried out on the basis of a generalized architectural description of IoT systems, taking into account the specifics of the subject area of use. The paper proposes a framework of a subject-oriented ontology to support security management of IoT systems.

Keywords

knowledge-based security management, ontology, cybersecurity, Internet of Things

1. Introduction

The IoT is becoming an increasingly important factor in ensuring sustainable development in various areas of human activity. When building IoT systems, the concept of a computer network of physical objects ("things") with built-in technologies for interaction with each other and the external environment is implemented [1–3]. The implementation of such networks allows influencing economic and social processes without human participation in performing individual actions and operations. IoT technologies provide dynamic adaptation to the context of the target system, collecting through the exchange and processing of data of the subject area, changing the processes of activity and the way of our life as a whole. [4]. IoT terms and definitions are presented in the ISO/IEC 20924 standard. This standard defines IoT as "an infrastructure of interconnected objects, people, systems and information resources together with intelligent services, allowing them to process information from the physical and virtual world and react" [5].

ITU-T Y.2060 recommendation notes that "from the perspective of technical standardization, the IoT can be viewed as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (ICT)" [6]. IoT is a cyber-converged system [7] that includes things, communication tools, target applications, and data analysis tools that support unique identification of each object. The growing scale and complexity of IoT systems, on the one hand, and security threats, on the other, require the development of security management tools taking into account the specifics of the domain of use. In 2017 was founded IoT Security Experts Group (IoTSEC) as an information exchange platform that brings together experts to ensure the security and resilience of the entire IoT ecosystem.

* CPITS-II 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2025, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
o.kovalenko@nubip.edu.ua (O. Kovalenko); natka_kn@ukr.net (N. Karevina)
0000-0002-9639-3544 (O. Kovalenko); 0000-0002-3291-8946 (N. Karevina)

IoT security organization issues are addressed in a large number of publications in this field of research and engineering from different perspectives. In particular, general issues of IoT security are discussed in [8, 9]. IoT security with the focus on the impact of emerging technologies outlined in [10]. Issues of forming security requirements for IoT components examines in [11, 12]. Security measures review for IoT is presented in [10]. A special place in research on ensuring IoT security is occupied by works focused on the use of formalized knowledge and ontologies [13–17].

[14] presents a general ontological model for security services based on the convergence of threats, vulnerabilities and risks of information assets. However, the model does not take into account the specifics of Internet of Things systems.

[15] introduced cybersecurity as one of the most important aspects of the full implementation of the IoT. Although the proposed approach does not take into account the aspects of risks and vulnerabilities.

[16] offers a basic ontology for the process of identifying and analyzing information systems security requirements. Although the impact of vulnerabilities is not specified and the specifics of the IoT are not presented.

[17] proposes the integration of vulnerabilities, weaknesses, methods, tactics, and attack models into a holistic set of relationships, but does not consider risks and intrusion models for the IoT.

Therefore, it is necessary to develop an ontological security model for the IoT that takes into account various security aspects and the relationships between the architectural components of the IoT.

The aim of this study is to develop an ontological model for IoT security management, taking into account threats, risks and intrusion patterns of IoT resources. The proposed approach is based on the architectural decomposition of IoT resources and the relationships between IoT components. The developed model for security management in IoT systems is based on the semantic interrelation between IoT domains and their influence on system functioning. The core idea is to converge different aspects of systems' safety into a single knowledge model with consideration of components and interrelations of IoT architecture.

2. IoT Components

Various sets (cases) of information, communication, and organizational technologies are used for the implementation of the IoT processes, which are necessary to solve the IoT tasks in the target subject area. The variety of components, the changeability of the problems of the system and the requirements for their solution require the task of quick adaptation of the system to solve current problems. The use of standard IoT design technologies may be unacceptable due to limited resources and the need for operational integration (convergence) of the requested IoT within the framework of a specific implementation (configuration) of the IoT ecosystem to solve current tasks.

The IoT ecosystem creates as set of independent constituent systems and technologies integrated into the principles of convergence. IoT components may be classified as architectural, process, and information.

3. IoT Architecture

The functional capabilities and properties of a separate IoT system configuration are determined by its architecture. System architecture is defined as a conceptual model that defines the structure, behavior and multiplicity of types (projections) of the system. Different types of system architectures are used to represent cybermatic systems, which can include IoT: software, organizational, technological, informational, process, etc. An architecture description is a formal description and presentation of a system, organized in such a way as to support conclusions (assumptions) about the structures and behavior of the system. The general description of the system architecture consists of three types of descriptions: structural, functional and organizational.

Software architecture is defined as the process of defining a structured solution that meets all technical and operational requirements while optimizing common quality attributes such as performance, security, and manageability. It involves a number of decisions based on a wide range of factors, and each of these decisions can have a significant impact on the quality, performance, maintainability, and overall success of the program.

IoT reference architecture, proposed in [18] is derived from a Conceptual Model and a set of characteristics that define a Reference Model and one or more architectural views. Characteristics of IoT systems are classified by three categories: architectures, trustworthiness, and functional. The IoT reference model presented as convergence of two contexts: entity-based and domain-based. In fact the IoT architecture include devices, communications, processing platforms, and use cases of big data analytics.

4. IoT processes

The main sense of IoT usage is decision-making on different layers of activity. Devices and objects with built-in sensors are connected to the IoT platform, which integrates data from various devices and applies analytics to share the most valuable information with applications created to meet specific needs. Powerful IoT platforms can determine exactly which information is useful and which can be safely ignored. The resulting information can be used to identify patterns, make recommendations, and identify potential problems before they occur.

As a constituent of decision-making processes IoT are implemented within the perceptual cycle and include stages of empirical awareness of the environment (target area), building and applying its model in the formation of rational behavior in the environment based on periodic updates of awareness of the current environment. Awareness of the state of the environment and the formation of rational behavior on its basis are carried out using the mechanisms of logical inference, corresponding to the stages of the perceptual cycle. Such mechanisms of logical inference in the cycle of situational interaction with the environment are abduction, induction, deduction and case based reasoning (CBR).

5. IoT Information

The formal description of the subject area of the IoT, for which a problem-oriented IoT is created, is a hierarchy of concepts (notions) and functional transformations that will be operated by users. The formal description of the subject area should also contain a generalized description of the IoT process model. The composition of IoT technologies should be carried out taking into account the architecture of the IoT [19–22].

Thus, the main task of the composition of components within the framework of the convergent architecture of the IoT can be defined as establishing the correspondence between the formal description of the application area and the means of information technologies:

$$B:(O,\ (D)\rightarrow(K,\ )L,M) \tag{1}$$

where B is the function of mapping model O of the subject area and model of requirements D to the problem-oriented IoT on the set of technological means (alphabet) of the IoT K and the set of control functions L of these technological means on the set M of admissible situations in the subject area.

The peculiarity of information technology is that its input and output is information that differs only in category, purpose, structure and content. Based on the category and purpose of input and output information of information technologies, it is possible to build their classification. In particular, information technologies can be distinguished by purpose:

- Registration and processing of primary signals
- Information structuring

- Cleaning of information
- Extraction, transformation and uploading of information
- Information analysis
- Mediation (visualization, voicing, clarification) of information
- Semanticization of information
- Formalization of semantics
- Assessments of the usefulness of information
- Building of constructive information models.

6. Model of IoT Security

The general approach to security management outlined in the standards is a risk-based approach. Therefore, the main goal of security management is to minimize risks. The ISO/IEC 27005 standard defines risk as "the impact of uncertainty on targets", and note 6 to this definition states: "information security risk is related to the potential opportunity for threats to exploit the vulnerability of an information asset or information assets and, therefore, cause damage to the organization". Furthermore, in the standard context of ISO/IEC 27005, "vulnerabilities may be associated with the properties of an asset that can be used in a manner or for a purpose other than that intended when the asset was acquired or manufactured". Simply put, a vulnerability is a weakness in an asset or group of assets that can be exploited by one or more threats, but a threat that does not have the corresponding vulnerability cannot cause a risk. And finally, "a risk assessment determines the value of information assets, the relevant threats and vulnerabilities that exist (or may exist), the controls in place and their impact on the identified risk, the potential consequences and, finally, the priorities of new risks and classify them according to risk assessment criteria established in the context of creation" [23]. The diagram shown in Figure 1 represents the dependencies between risks, threats, vulnerabilities, and information assets.

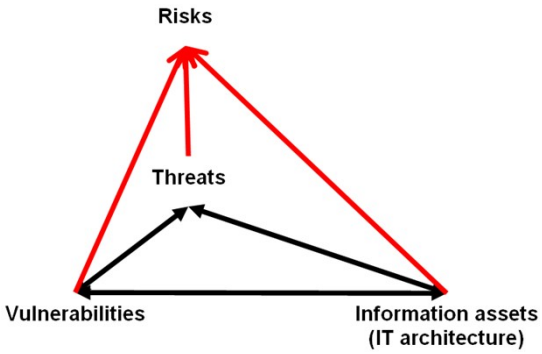

Figure 1: Dependencies between risks, threats, vulnerabilities and information assets

Risk assessment is the basis of security management and the use of an adequate set of security models. Information assets are parts of the IT architecture. Therefore, when evaluating information assets, we consider these assets as an instance (variant) of the IT architecture. The model describes risk factors related to threats, vulnerabilities and IT architecture [14].

The convergent knowledge model of information security management is implemented based on the knowledge models of risk components (Figure 1). The ontological model of knowledge of the subject area allows describing the main concepts (propositions) of the subject area and defines the relations between them. The process of building ontologies includes:

- classes and their properties (classes, properties).
- properties of each concept, which describes various functional capabilities and attributes of the concept (clots (slots), sometimes called roles).

- slot restrictions (also known as slot facets, sometimes called role restrictions). The ontology together with many individual instances of classes make up the knowledge base.

Model of information security management for IoT is presented as tuple

$$T = (A,\ P, I, R, C, F), \tag{2}$$

where A is an IoT architecture model; P is a processes model in IoT system; I is an information model of IoT system; R is a risks model of IoT system; C is a connectivity model; F is a model of information interpretation in IoT system.

A fragment of IoT security ontology is depicted in Figure 2. The notions of security and privacy by default and security and privacy by design naturally emerge as being foundation cornerstones of IoT security. Evidently, it is challenging to apply these concepts in several different environments that will have particular characteristics. In IoT the cyber risk is context-dependent (i.e. based on the application scenario) and in this respect the principles of security and privacy by design should be applied with this consideration in mind. Following relevant initiatives from other, more mature IT sectors can prove to be beneficial in adopting such principles for the IoT ecosystem.

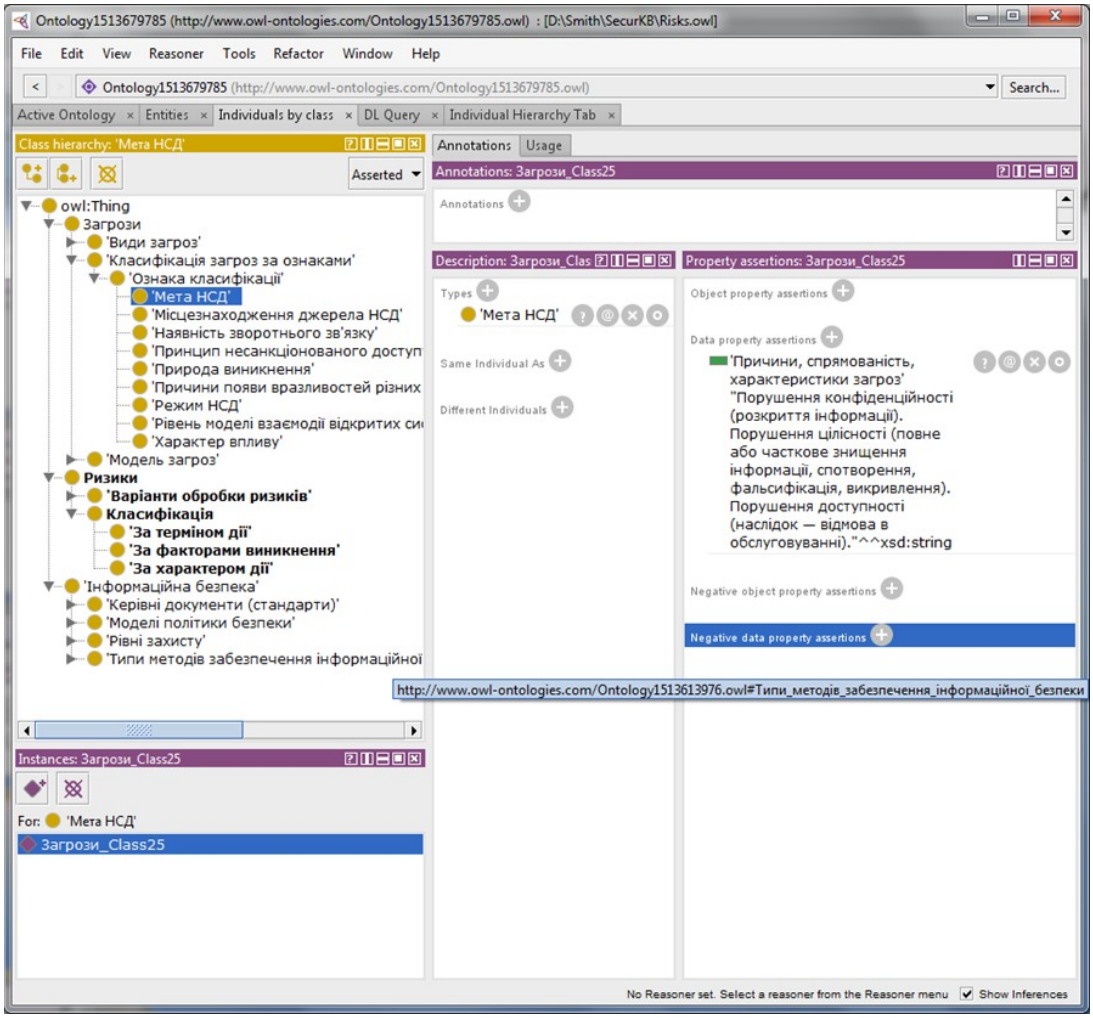

Figure 2: Security ontology fragment

Establishing correspondence between the formal description of the subject area and the means of IoT allows applying a knowledge-oriented approach to the development of IoT. The proposed approach ensures the formation of a repository and the convergence of IoT tools to solve the target problems of IoT security management through the composition of the stages of ontological analysis of requirements, functional decomposition, subject interpretation and physical implementation.

The use of the proposed model of the design process will allow providing a formalized synthesis of IoT for the target subject area through the convergence of the necessary IoT components based on knowledge models. Complex IoT systems have a multi-level structure, with the distribution of system functions and services by levels in accordance with their purpose.

7. Conclusions

The proposed ontological model of IoT security converge different aspects of safety in context of components IoT architecture. The diversity, heterogeneity, complexity and spatial distribution of IoT systems cause corresponding difficulties in building their security systems. The application of a knowledge-oriented approach allows you to speed up the process of designing security tools for IoT, taking into account the specifics of their field of application based on a generalized ontology. The proposed framework defines the components of the IoT model as generalized classes that can be detailed by specific scope concepts. Generalized ontological classes of architecture, processes, information, and risks are used to represent the IoT ecosystem. Each of the generalized classes can be specified by appropriate target subclasses and domain concepts. The developed framework can be used when building a target IoT with appropriate security means.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] V. Lakhno, et al., Management of Information Protection based on the Integrated Implementation of Decision Support Systems, East.-Eur. J. Enterp. Technol., vol. 5, no. 9(89), 2017, 36–41. doi:10.15587/1729-4061.2017.111081

[2] P. Skladannyi, et al., Model and Methodology for the Formation of Adaptive Security Profiles for the Protection of Wireless Networks in the Face of Dynamic Cyber Threats, in: Cyber Security and Data Protection, vol. 4042 (2025) 17–36.

[3] Y. Kostiuk, et al., Effectiveness of Information Security Control using Audit Logs, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3991, 2025, 524–538.

[4] The European Union Agency for Cybersecurity, Baseline Security Recommendations for IoT, 2017. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[5] ISO/IEC 20924:2024. Internet of Things (IoT) and Digital Twin—Vocabulary, 2024. https://www.iso.org/standard/88799.html

[6] ITU-T, Y.2060: Overview of the Internet of Things, Technical Report, International Telecommunication Union, 2012. https://www.itu.int/rec/T-REC-Y.2060-201206-I

[7] O. Kovalenko, Knowledge Driven Cyber-Convergent Systems based on Situational Agents, in: 2022 IEEE 17th Int. Conf. on Computer Sciences and Information Technologies (CSIT), 2022, 243–246. doi:10.1109/CSIT56902.2022.10000762

[8] B. Alotaibi, A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities, Sensors, 23 (2023) 7470. https://doi.org/10.3390/s23177470

[9] V. Mullet, P. Sondi, E. Ramat, A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0, in: IEEE Access, 9 (2021) 23235–23263. doi:10.1109/ACCESS.2021.3056650

[10] P. Williams, I. K. Dutta, H. Daoud, M. Bayoumi, A Survey on Security in Internet of Things with a Focus on the Impact of Emerging Technologies, Internet of Things, 19 (2022) 100564. doi:10.1016/j.iot.2022.100564

[11] G. Ogunniye, N. Kökciyan, A Survey on Understanding and Representing Privacy Requirements in the Internet-of-Things, J. Artificial Intelligence Res. 76 (2023) 163–192. https://jair.org/index.php/jair/article/view/14000

[12] A. Souag, R. Mazo, C. Salinesi, I. Comyn-Wattiau, Using the AMAN-DA Method to Generate Security Requirements: A Case Study in the Maritime Domain, Requirements Eng. 23(4) (2018) 557–580. doi:10.1007/s00766-017-0279-5

[13] J. S. Rueda-Rueda, J. M. T. Portocarrero, Framework-based Security Measures for Internet of Thing: A literature Review, Open Comput. Sci., 11(1) (2021) 346–354. doi:10.1515/comp-2020-0220

[14] O. Kovalenko, T. Kovalenko, Knowledge Model and Ontology for Security Services, in: IEEE 1st Int. Conf. on System Analysis & Intelligent Computing (SAIC), 2018, 1–4. doi:10.1109/SAIC.2018.8516875

[15] B. A. Mozzaquatro, R. Melo, C. Agostinho, R. Jardim-Goncalves, An Ontology-based Security Framework for Decision-Making in Industrial Systems, in: 4th Int. Conf. on Model-Driven Engineering and Software Development (MODELSWARD), 2016, 779–788.

[16] A. Souag, C. Salinesi, R. Mazo, I. Comyn-Wattiau, A Security Ontology for Security Requirements Elicitation, in: Engineering Secure Software and Systems (ESSoS), 2015, 157–177. doi:10.1007/978-3-319-15618-7_13

[17] S. Zhang, et al., Multi-Source Knowledge Reasoning for Data-Driven IoT Security, Sensors, 21 (2021) 7579. doi:10.3390/s21227579

[18] ISO/IEC 30141:2024 Internet of Things (IoT)—Reference Architecture, 2024. https://www.iso.org/standard/88800.html

[19] V. Dudykevych, et al., Platform for the Security of Cyber-Physical Systems and the IoT in the Intellectualization of Society, in: Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 449–457.

[20] B. Zhurakovskyi, et al., Secured Remote Update Protocol in IoT Data Exchange System, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 67–76.

[21] O. Shevchenko, et al., Methods of the Objects Identification and Recognition Research in the Networks with the IoT Concept Support, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 277–282.

[22] V. Sokolov, et al., Method for Increasing the Various Sources Data Consistency for IoT Sensors, in: IEEE 9th Int. Conf. on Problems of Infocommunications, Science and Technology (PICST) (2023) 522–526. doi:10.1109/PICST57299.2022.10238518

[23] ISO/IEC 27005:2022. Information Security, Cybersecurity and Privacy Protection—Guidance on Managing Information Security Risks, 2022. https://www.iso.org/standard/80585.html