Context-Defined Model of Open Systems Interaction for IoT Cybersecurity Issues Study

Victor Tikhonov[1], Eduard Simens[2], Yevhen Vasiliu[1], Valery Sitnikov[3], Abdullah Taher[4], Olena Tykhonova[1], Kateryna Shulakova[1,2] and Serhii Tikhonov[3]
[1]*Department of Information Technologies and Cybersecurity, State University of Intelligent Technologies and Telecommunications, Kuznechna Str. 1, 65023 Odesa, Ukraine*
[2]*Anhalt University of Applied Sciences, Bernburger Str. 57, 06366 Köthen, Germany*
[3]*Department of Computer Systems, Odesa Polytechnic National University, Shevchenko Avenue 1, 65044 Odesa, Ukraine*
[4]*Department of Electronic and Communication Engineering, College of Engineering, Al-Qadisiyah University, Babilon Str., 29, 58002 Al Diwaniyah, Iraq*
victor.tykhonov@gmail.com, olena.tykhonova@suitt.edu.ua, ye.vasiliu@gmail.com, sitnvs@gmail.com, abdallahqays@gmail.com, katejojo29@gmail.com, od.sergii.tihonov@gmail.com

Keywords: Internet of Things, Open Systems and Networks, General System Theory, Cybersecurity, Context-Defined Model.

Abstract: The article considers the issues of IoT systems and networks privacy. The complex researches on general system theory state of the art has been surveyed, as well as cybersecurity aspects of IoT technologies and models analyzed over the past decades with respect to the Industry 4.0 concept and industrial IoT architecture. A comprehensive decomposition formalism proposed on the base of M. Mesarowic system theory for presenting the complex cybersecurity object of study as a set of its parts. An original context-defined model of open systems interaction S-CDM has been constructed for cybersecurity issues study with the use of J. Neumann classification and A. Uemov system triad. The S-CDM model is shaped in 3-layer hierarchical graph. The first S-CDM layer displays the cybersecurity problem as a set of relations between the key players of information market – resources, clients and agents. The second S-CDM layer adds the network technologies impact on the relations between the key market-players. The third S-CDM layer includes a "degree of trust" factor into the key market-player relationships. The introduced context-defined model enables to reduce the overall problem complexity of the IoT cybersecurity study to a number of less complex and easy-handled partial tasks. As an example, a particular local version of the S-CDM model is considered in the form of six independent tasks for AI-aided methods of cybersecurity provision. The results of the work intend to contribute general system researches in the sphere of network system modelling and IoT privacy.

1 INTRODUCTION

Many challenges in modern society require a deep understanding of systems characterized by a large number of components, for which the constituent's concerns (atoms, cells, devices, individuals, organizations) are accompanied by the issues of their interactions study. Typical examples are nuclear physics, knowledge organization, global computer networks and Internet of things (IoT).

Holistic approach to such objects implies construction some relevant model of open system parts intercaction, dependent on researcher subject objectives. Because of that, different concurrent models of similar objects have right to exist and implement.

For instance, the Standard Model of particle physics provides a uniform theory to electromagnetic, weak, and strong interactions. Modern knowledge categorizing systems use three models: hierarchical, faceted, and enumerative. The contemporary Internet model has gone from initial OSI reference model and the TCP/IP protocol suite up to the ultimate Industrial Internet architecture framework.

One of the main goals of constructing a model of a complex object is to reduce the overall problem complexity when tearing it into several relatively independent and more simple tasks. This is not yet a problem itself solution, but the first step to get it.

An important large object of systematic study in recent years is the IoT architecture in the context of information privacy.

This work focuses the IoT privacy issues as a complex cybersecurity problem, and intends to find its comprehensive decomposition on the base of general system theory and Internet of things architecture analysis, in order to convert down the problem into a set of interconnected partial tasks of less complexity.

In the scope of this work, an object **O** model is considered as a subject' **S** personal point of view on the object of his study understood as a "closed-open substance" connected both to open subject **S** and open environment **W**. It means, that an abstract model of a real object is supposed to some extent subjective, while its relevance can be proven empirically.

So, an "open system" is defined as a subject-view function **S(O, W)**, where object **O** consist of a set of things $\{\mathbf{T_n}\}$ interacting to each other, or somehow with its open environment **W** through the subject **S**, and possibly directly with **W**.

The Internet itself is conventionally studied as a large open network formed by open sub-networks interacting via common protocols and interfaces. The global Internet project was created as a union of autonomous systems, networks and independent manufacturers of network equipment, without centralized system administration, built-in security mechanisms and real-time big data management.

Adaptation to new requirements often followed the way of "patching holes" when protocols` amendments and changes superimposed on their previous modifications, which ultimately led to cybersecurity issues due to unbridled Internet complexity increase and unclear consequences of AI rapid advances.

In the process of network technologies evolution, various reference models of Internet open systems interaction have been proposed, including the first well-known 7-layer OSI/ISO reference model and the ultimate 3-layer reference IoT model developed by Industrial Internet Consortium (IIC); these models reflect different visions of Internet architecture, and to one degree or another, continue to be used.

Section 2 of this work surveys researches on complex systems and networks.

Section 3 formulates motivations and objectives of the work.

Section 4 analyses the cybersecurity aspects in the IoT technologies and models with respect to "Industrial IoT" (IIoT) specifications as a key component of the Industry 4.0 concept.

Section 5 constructs a context defined model of open system interaction with the use of J. Neumann classification and A. Uemov system triad for the IoT cybersecurity issues study.

Sections 6 and 7 summarize the work's discussion and conclusions.

2 COMPLEX SYSTEMS AND NETWORKS RESEARCHES. STATE OF THE ART

Large-scale project development, such as those involving the Internet, often requires breaking down complex tasks into sequential stages. Systems, whether natural or artificial, typically follow a life cycle with stages like initiation, development, and conclusion. In system theory, this cyclic evolution is seen as a fundamental phenomenon where the end of one phase often leads to the beginning of another.

In contrast to biological systems, technical systems often evolve through incremental improvements, gradually adapting to new conditions or needs, which can eventually lead to increased complexity and potential instability. This process highlights the importance of structured design principles to manage the growth of these systems.

To ensure compatibility and coherence between various components of a project, it's crucial to establish a unified system architecture. This architecture formalizes the properties and interaction protocols of the different elements. Employing a systematic approach with a focus on modular design enables the decomposition of complex systems into simpler, interrelated components.

Modern system analysis methodologies, such as object-oriented tools and modelling techniques, support this structured approach. By focusing on phases like planning, analysis, design, and implementation, these methodologies aim to create new value through systematic development and optimization [1].

In his work "Systemology. General Theory of Systems" A.E. Kononyuk notes the importance of forming a professional language of systems analysis, including the choice of an adequate system of concepts and relevant terminology (names), considering the peculiarities of their intuitive interpretation in various natural languages (German, English, etc.). It is proposed to widely use terms in their established meaning, which can only be clarified; orientation towards the terminology of fundamental sciences (primarily mathematics); use, if possible, of international terminology [2].

The attribute "general" of system theory itself is clarified as "the most essential, characteristic of all

the foundations of something". Two main classes of problems identified: system analysis and synthesis. Emphasized, that rapid growth of information would be catastrophic for the further development of human cognition if no generalized knowledge occurred along with the expansion and deepening of sciences [2].

In recent years, systems analysts have increasingly focused the methods of big data processing, artificial intelligence (AI) and machine learning (ML) when using the systems theory as a math-superstructure to the theory of learning (both machine and human), connecting them with model-based system design practice. The set-theory seen as a formal framework for general system knowledge with the details of learning theory [3].

The enterprise model as an open system is considered by K. Lang & Co, aiming to create a framework for digital transformation: a system is self-contained; consists of subsystems, inputs, and outputs; and is in constant change. Systems arise through the determination of a barrier, which enables the distinction between the system and its environment. The elements inside a system, the organization comprising structures and processes, people and technologies or equipment all influence each other mutually, and the system only has meaning through the interaction of the elements. The system includes 6 items: business model, input data, supplier interface, company, services, client interface [4].

In October 2023, the USA President's Council (PCAST) published report "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" which assessed the AI capabilities and its open human-environment to address the major global challenges. When supervised properly and responsibly by human experts, trained on high quality data, and verified using reliable scientific techniques, "AI tools can become engines of innovation that can supercharge the ability of scientists and policymakers to address such challenges". To achieve these goals, advanced models, data sets, and benchmarks need to be broadly available to the scientific community.

Though, AI can create new challenges (distilling errors and biases embedded in skewed training data, enormous energy for computation, the possibility that faulty science could be unwittingly generated, and the ease with which nefarious actors could use new powerful AI technologies for malicious purposes. The ideal future of AI-enabled science will require continued attention in three areas: empowerment of human scientists; responsible use of AI tools; sharing of basic AI resources. The experts formulated basic recommendations: expand efforts to secure access AI resources to federal data sets for approved critical research needs; support basic and applied AI researches across academia, industry, national labs and federal agencies; adopt responsible and transparent AI-use throughout all stages of the scientific research process; encourage innovative approaches to integrate AI-assistance into scientific workflows [5].

3 MOTIVATION AND OBJECTIVES OF THE WORK

In the modern era of Internet of Things (IoT) and global instability, information security became one of the most pressing issues, that includes various aspects of storing, accessing and transmitting large volumes of confidential data. It belongs to the objects of complex systems and networks study surveyed above in Section 2.

To date, solid results have been achieved in systems analysis and design. Based on G. Kron diakoptics, M. Mesarovic method and L. von Bertalanffy general systems theory (GTS), various models of system-decomposition can be constructed to reduce the initial object's complexity as a first step to approach a problem. However, this is not a trivial engineering task but somehow a creativity art.

One of the long-known principles of hierarchical decomposition and ordering of complex things is indexing classes of things by integers, e.g., Universal Decimal Classification (UDC). Though, the non-trivial matter is – which base of the number system is better to use (10, 8, etc.), and how to define semantic classes at each level of hierarchy.

J. Neumann gave a rigorous answer to the first question: ternary integer numbering for abstract things ordering is optimal in terms of information capacity. The Mesarovic method lets formally obtain relations sets on the given classes of things in accordance with A. Uemov system triad "Things, properties, relations".

Thus, the core non-trivial task in complex object decomposition is the relevant definition of interconnected semantic classes of things with respect to given problem study. This motivation idea underlies our objectives and discussions in this work.

The work aims system decomposition of the complex IoT cyber security problem in multiple fewer complex tasks as a first step to approach the problem.

To achieve this goal, the following objectives are set in the work:

1) Analysis the cyber security aspects of basic IoT technologies and models with particular focus on the USA NIST SP 800-183 specification and Industrial IoT Connectivity Framework.

2) Construction a context-defined model of open systems interaction for the Internet of things cyber security problem study on the base of J. Neumann ternary classification and A. Uemov system triad.
3) Interpretation the obtained context-defined model in a particular case-study of the artificial intelligence-based cybersecurity provision.

4 CYBERSECURITY ASPECTS IN THE IOT TECHNOLOGIES AND MODELS

The problem of cybersecurity is largely due to the rapid development of sensor network technologies and the growth of the IoT segment in the overall Internet infrastructure [6].

Germany played a leading role in foundation of basic IoT technologies and development the concept of future industry – "Industry 4.0". In 1980s began the rise of classic Fieldbus technology with proprietary serial protocols from some German manufacturers, aiming to reduce the installation and maintenance effort of industrial machines and systems. It was an industrial network system for real-time distributed control to connect instruments in a manufacturing plant. A Fieldbus works on networks of diverse topologies (daisy-chain, star, ring, branch, tree etc.). In 1987, the Process Field Bus (ProfiBus) was launched through a publicly funded project by companies and institutes [7].

Based on these advances, one of the first IoT technologies M-Bus was developed in 1991 by H. Ziegler from Paderborn Univ., in coop with Texas Instruments GmbH and Techem GmbH for remote reading of utility meters (water, gas, electricity and heat). M-Bus was initially standardized in EN1434 for thermal energy meters and then defined in EN13757x specifications family issued by the EC committee CEN since 2002: EN 13757-1 (2002-2022) – generic descriptions for communication systems; EN 13757-2 (2004-2018) – wired OSI PHY and DL layers; EN 13757-3 (2005-2018) – dedicated OSI APP layer. The PHY layer supports galvanic-type asynchronous interface on 2-core copper cable. In 2003 the wireless M-Bus was deployed (EN 13757-4, 2008-2019) [8].

In 1998, the Connectivity Standards Alliance (CSA, formerly Zigbee Alliance), after the Bluetooth (1994) and Wi-Fi (1997) technologies emerged, created ZigBee-technology for automated data collection from IoT devices around 10-100 m at ISM (Industrial, Scientific, Medical) radio frequencies 900/868 MHz and 2.4 GHz. It has low power consumption and data transfer rate (20-250 Kbit/s), but a high level of data protection (AES with 128-bit symmetric key); still, it took off only in 2002 when more interested companies joined the Zigbee Alliance, [9]. Related standard IEEE 802.15.4 was firstly adopted in 2003 and ratified by ZigBee in 2004; then it was revised to Zigbee_Light_Link library (2006) and ZigBee Pro/2007 revision [10].

In 2012, the *first* IoT reference 4-layer model of ITU (Y.400/Y.2060) was issued [11]. In 2014, the *second* reference 7-layer IoT architecture was adopted by the IoT World forum [12], [13].

In June 2016, the ISO specification 20922 was published for Message Queuing Telemetry Transport protocol (MQTT), that has become the de-facto standard for Industry 4.0 concept (manufacturing modernization projects and digital transformation of the field, real-time decision making, enhanced productivity, flexibility and agility) [14]. In July 2016, the *third* IoT reference 4-layer model was issued by the USA National Institute of Standards and Technologies (NIST SP 800-183) with particular accent on the IoT security issues [15].

The MQTT standard, along with the NIST SP 800-183 IoT-architecture (2016), opened a new stage in the development of IoT technologies known as "Industrial IoT" (IIoT) – a key component of the Industry 4.0 concept. The history of the IIoT begins with the invention of the programmable logic controller (PLC) by R. Morley (1968), which was used by General Motors in automatic transmission manufacturing. These PLCs allowed for fine control of individual elements in the manufacturing chain.

The term "IIoT" was coined in the USA, it covers parts of the overall Industry 4.0 concept ([7]). Now, the "IIoT" means extension the IoT paradigm into industrial settings and applications via internet IP-connectivity to integrate advanced sensors, software, and machinery aimed for collecting, analyzing and processing upon vast amounts of data. This data-driven approach enables real-time decision-making and predictive analytics, leading to enhanced operational efficiency, reduced costs, and improved product quality [17]. In accordance with that, in 2017, the 802.15.4 ZigBee standard was extended up to over IP running version by the Dotdot (//:) library ([18], [19]); its current revision (2020) supports wireless personal area network (WPAN) of ad-hock mesh topology [20].

In 2022, the Industry IoT Cons. (aka Industry Internet Cons. IIC™, now integrated into the Digital Twin Cons. DTC™) published "The Industrial IoT Connectivity Framework" (IIC-model), where the IIoT interoperability presented by 3 layers (technical

end devices, syntactic IIoT platform, semantic human/AI users), [21], [22]. This document presents the currently *ultimate (number four)* 3-layered reference model of the IoT. One of the popular today IIoT development platform is a virtual EMQX broker, that was designed by EMQ company; it supports protocols MQTT (3.1, 3.1.1, and 5.0), HTTP, QUIC, and WebSocket for up to 100 million concurrent IoT devices per cluster with 1 million messages per second and a millisecond latency [23].

Consider the cybersecurity context of IoT, take in account the following related aspects. 1) The IoT networks operate vast amounts of sensitive data, ranging from personal information to critical business data. 2) Many IoT-segments are imbedded in critical infrastructure like power grids, water supply and transportation. 3) The IoT systems widely use vulnerable wireless links [24]. E.g., ZigBee standard permits re-use of link keys for re-joining the network; so an attacker can clone the legitimate device and spoof the network layer of Trust Centre by pretending to be previously connected device wanted to re-join the network [25]. 4) Recently, AI has played an increasingly important role in Big Data processing around the IoT segments; on the other hand, this opens up negative opportunities for malicious use of new AI-researches.

The above ITU model of IoT (2012) defines 4 layers: devices, network transport, service platform and applications. Two kinds of security capabilities declared: generic ones (authorization, authentication, data integrity protection, access control etc.) and IoT-specific options (without concrete details).

The next spoken above IoT/WF model (2014) defines 7 layers: (IoT devices, connectivity, edge cloud computing, data accumulation, data aggregation, applications, business processes). Those years exhibited an extensive growth of IoT segment, so, this model had primarily warred about technological aspects of Big Data management. The IoT privacy had not attracted enough attention then; as a result, serious problems arose.

To address emerging IoT privacy concerns, NIST introduced an IoT reference model (SP 800-183) in 2016. It defines 4 abstract layers in the context of privacy provision: sensor clusters with individual impact weights d_i; aggregators that implement summation $\mathrm{Sum}(d_i)$; communication channels (e.g., USB, wireless, wired, verbal etc.) incl. those offering as a service (AAS); external AAS-utilities (eUtilities) where a human may be viewed as an eUtility-service.

Data supplied by an eUtility can be weighted. Non-human eUtility may have device ID, which can be crucial for identification/authentication. The key role in this model play the so-called "decision-making triggers" (DTs) acting at any layer and formalizing the primary goal of the IoT on the upper layer (eUtility). The overall IoT network framework upon this model is similar to a spatially distributed artificial neural network. Herewith, the complex system problem of IoT cybersecurity is functionally decomposed on four distinct tasks of reduced complexity according to defined 4 layers of the model.

The 3-tier IIC-model (2022) spoken above addresses the “Industrial Internet Reference Architecture” IIC-IIRA [26] and “Industrial Internet Security Framework” IIC-IISF [27]; these three documents currently most fully and systematically describe the overall IIoT-architecture and the general concept of cybersecurity in modern digital world.

The IIC-model follows OSI/ISO and TCP/IP: OSI layers L1÷L4 have been merged in a transport **T** tier for delivering TCP/UDP messages (technical interoperability **TchIO**); layers L5÷L7 merged/split for data framework **F** (files of state or events formed by messages – syntactic interoperability **SinIO**); document **D** – the context-interpretation of **F** (Semantic interoperability **SemIO**).

TchIO means information exchange (bits/bytes, e.g. pencil scribbles), assuming that info-exchange structure (e.g. pencil and paper) established. SinIO means info-exchange in a common data structure (e.g., in a known language grammar). SemIO is unambiguous context-appropriate interpretation of exchanged data.

The IIC-IIRA (2022) comprises 3 tiers: edge (IoT access network), Internet-based service platform and enterprise API/human ([25], page 44). It is close to previously discussed 4-tier NIST SP 800-183 model, if communications combined with service platform. This breaks a typical IoT-domain in 3 interacting parts with 3 individual responsibilities (edge, platform, API) and 3 interoperability ones: “edge-platform”, “edge API”, “platform-API”; these responsibilities include security aspects (both IT- and OT-types).

The IIC-IISF (2016) provides guidance for trustworthy systems, security characteristics, technologies and techniques to be applied, and how to gain assurance that the appropriate mix of issues have been addressed to meet stakeholders' expectations. The core term “Trustworthiness of an IIoT System” is defined as a unit of 5 entities (resilience, reliability, safety, privacy, security) which are exposed to 4 external influences: environment disruption, system faults, attacks, human errors ([25], p. 23).

Key factors of IIoT security are focused therein: convergence of IT and operational technology OT (p.

24); evolution of IT and OT security ([25], p. 25); brownfield (new + legacy) deployments in OT (p. 26); in a typical IIoT system, cloud computing is supposed a critical point of vulnerability as using a shared third-party service-providers creates a number of trust boundaries affecting security and privacy ([25], p. 27); functional breakdown noted for security model and policy ([25], p. 59).

5 CONSTRUCTION A CONTEXT DEFINED MODEL FOR CYBERSECURITY STUDY

The Internet has been around for about half a century, and as its technologies have evolved, various reputable organizations have introduced at least 7 different functional models of the Internet open systems interaction, starting with OSI reference model and TCP/IP protocol suite in late 1970s.

It is important to note that each newly emerging model of network architecture did not reject the previous ones, but rather complemented and developed them in the context of new specific objectives. Therefore, all these models, one way or another, continue to be used by specialists. The seven-layer OSI/ISO reference model defines commonly popular professional terms of an abstract open system, while the four-layer TCP/IP stack formulates detail interfaces of real network objects interaction. The three-layer NGN/ITU model maps any open packet-based network (incl. entire Internet) in a pretty simple view: transport infrastructure (lower level) and application domain (upper level), which counteract via IP protocol (middle level).

The last four models (2012, 2014, 2016, 2022) have been developed for IoT-networks architecture; among them, NIST SP 800-183 (2016) model was a response to the cybersecurity challenge, and the ultimate IIC-model (2022) together with IIC-IIRA and IIC-IISF, form a holistic vision of the modern Industry 4.0 concept.

Thus, it is concluded, that a holistic approach to a complex problem needs construction a specific model of this problem in the context of the objectives posed by the researcher.

Let's introduce a context defined model (CDM) of open system interaction between clients **C**, resources **R** and agents **A** via network **N**, Figure 1.

The object **R** in Figure 1 means a set of *information resources* which are commonly accessible on the market; the object **C** symbolizes a set of *clients* of the info-resources market; **A** is a set of *broker-agents* on the info-resources market.

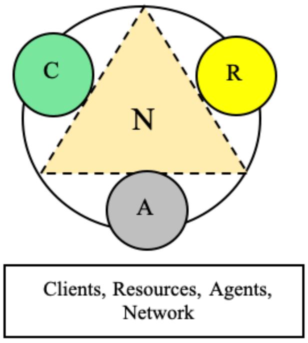

Figure 1: "Client-Resource-Agent" context defined model of open system interaction (CDM).

Objects (**R**, **C**, **A**) may interact directly in pairs (**R**,**C**), (**R**,**A**), (**C**,**A**) or/and via the *network* communication media **N**. Each of the objects (**R**, **C**, **A**) is a unit of two subsets: $\mathbf{R}=(\mathbf{R}_T, \mathbf{R}_F)$; $\mathbf{C}=(\mathbf{C}_T, \mathbf{C}_F)$; $\mathbf{A}=(\mathbf{A}_T, \mathbf{A}_F)$, where $(\mathbf{R}_T, \mathbf{C}_T, \mathbf{A}_T)$ are authorized (*true*) objects; $(\mathbf{R}_F, \mathbf{C}_F, \mathbf{A}_F)$ – unauthorized (*fake*) objects.

At the first two steps of security-problem decomposition, a set **S** of six relationships can be constructed:

$$\mathbf{S}:=\{\mathbf{S_i}\} = \{[(\mathbf{R},\mathbf{C})_1, (\mathbf{R},\mathbf{A})_2, (\mathbf{C},\mathbf{A})_3], [(\mathbf{R},\mathbf{C})_{N4}, (\mathbf{R},\mathbf{A})_{N5}, (\mathbf{C},\mathbf{A})_{N6}]\}, \quad (1)$$

where relationships like (x, y) in (1) may be defined either commutative (symmetric) or non-commutative (asymmetric). The symmetric case of relationships **S** in (1) presents the adjacency matrix graph in Figure2.

S	R	C	A	N
R		1	1	1
C	1		1	1
A	1	1		1
N	1	1	1	

Figure 2: Symmetric adjacency matrix graph of S.

At the third step, the following commutative or noncommutative Cartesian products can be defined:

$$\begin{cases} (\mathbf{R},\mathbf{C})_1 \rightarrow (\mathbf{R}_T,\mathbf{C}_T)\times(\mathbf{R}_F,\mathbf{C}_F); \\ \dots\dots\dots\dots\dots \\ (\mathbf{C},\mathbf{A})_3 \rightarrow (\mathbf{C}_T,\mathbf{A}_T)\times(\mathbf{C}_F,\mathbf{A}_F); \\ (\mathbf{R},\mathbf{C})_{N4} \rightarrow (\mathbf{R}_T,\mathbf{C}_T)_N \times(\mathbf{R}_F,\mathbf{C}_F)_N; \\ \dots\dots\dots\dots\dots \\ (\mathbf{C},\mathbf{A})_{N6} \rightarrow (\mathbf{C}_T,\mathbf{A}_T)_N \times(\mathbf{C}_F,\mathbf{A}_F)_N. \end{cases} \quad (2)$$

The bipartite graph of a commutative Cartesian product for $(\mathbf{R},\mathbf{C})_1$ for direct relationships member in (2) presents Figure 3.

S_1	R_F	C_F
R_T	(R_T, R_F)	(R_T, C_F)
C_T	(C_T, R_F)	(C_T, C_F)

Figure 3: Bipartite graph of Cartesian product for $(R,C)_1$.

In the scope of this work, the CDM model (Fig. 1) along with decomposition formalisms (1) and (2) is accepted as the *cyber Security Context-Defined Model* (S-CDM).

The security context-defined model S-CDM can be presented by a 3-layer hierarchical graph shown in Figure 4.

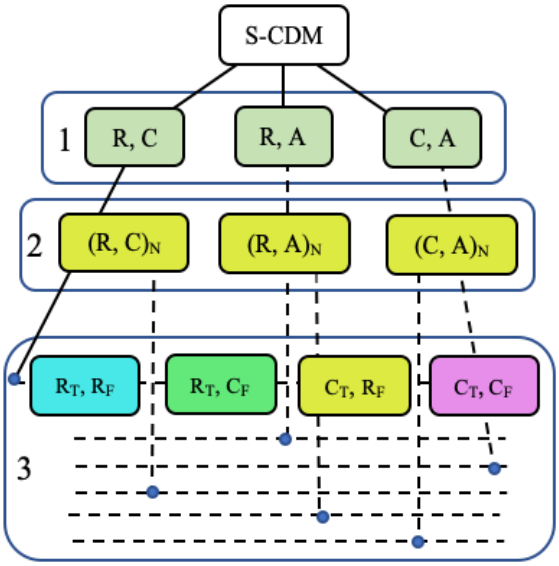

Figure 4: The graph of security context-defined model.

The *first layer* in Figure 4 (denote it S-CDM1) displays the cybersecurity problem decomposition as a set of three types of relationships between the three key objects: **R** (information resources on the market), **C** (customers of the information resources), **A** (intermediary agents, or brokers, on the information resources market). Here the S-CDM1 is understood in two different aspects: a) in a *narrow sense*, as a system of regulatory and legal relations between three key players on the information market (**R**, **C**, **A**) – with a direct mechanism of interaction (ignoring the network issues, illegal or criminal objects impact, hacker attacks, etc.); b) in a *broad sense* (considering the influence of various counteracting or harmful factors).

The *second layer* in Figure 4 (S-CDM2) adds network media (N) as a significant operational factor in relationships between the key players (R, C, A) on the information market. Joint accounting of S-CDM1 and S-CDM2 is considered next as a partial extension of the S-CDM1 model (in its narrow sense) with respect to cybersecurity problem. Herewith, the S-CDM2 layer splits each of the S-CDM1 tasks in two related distinct tasks which consider or not the network interaction impact.

The *third layer* in Figure 4 (S-CDM3) includes the logical category "degree of trust" into 6 relations of layer 2 between the key players (**R**, **C**, **A**) on the information market.

Thus, each of the six S-CDM2 layer relations splits into 4 classes at the S-CDM3 layer according to (2) and Figure 3. The four of S-CDM3 classes split by $\mathbf{S_1}=(\mathbf{R},\mathbf{C})_1$ are explicitly shown in Figure 4 as $\{(R_T, R_F), (R_T, C_F), (C_T, R_F), (C_T, C_F)\}$; the rest five ones are outlined implicitly. As a result, the context-defined model S-CDM (Fig. 4) of cybersecurity problem decomposition concludes 24 elementary tasks at its bottom layer.

The introduced above S-CDM-model for hierarchical decomposition of relationships between the key information market players (**R**, **C**, **A**) enables setting various cybersecurity relevant tasks of systems analysis and synthesis by presentation the S-CDM model in different structural bases. Below, two examples of such structural bases are exhibited.

Basis 1. Regulatory/operational cybersecurity. The cybersecurity problem is presented by three orthogonal structural primitive branches (Fig. 5). There are three independent tasks that can be raised up on this S-CDM model; each of them includes two nested sub-tasks. This basis is convenient for studying the cybersecurity problem ignoring the third parties aggressive influence.

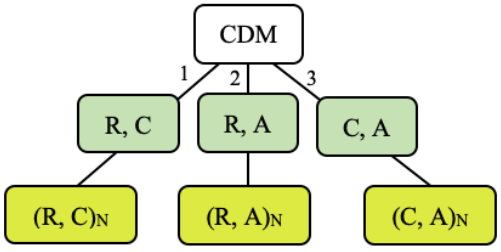

Figure 5: Regulatory/operational cybersecurity model.

Basis 2. Fake-agents on the info-market.

The cybersecurity problem is presented by two orthogonal primitive branches – independent tasks (Fig. 6); each of them includes four nested sub-tasks.

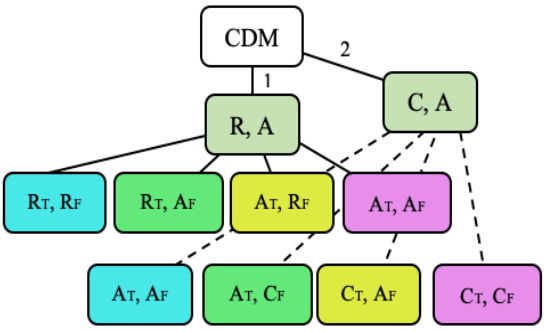

Figure 6: Fake-agents on the info-market model.

The S-CDM-approach can be used to approach the cumbersome issue of AI-application in the IoT cybersecurity provision through decomposition the object of study into less complex partial tasks.

Let "**( )**" be common regulatory/operational (RO) tools; "**( )$_{AI}$**" – particular AI-aided RO-tools; "**ID**" – *identifications*; "**AU**" – *authorizations*; "**VR**" – *verifications* (e.g. authentications).

Let define a local cybersecurity model:

$$\text{S-CDM}_{CS} := [\mathbf{(\,)}, \mathbf{(\,)}_{AI}] \times [\mathbf{C}, \mathbf{R}] \times [\mathbf{ID}, \mathbf{AU}, \mathbf{VR}]. \quad (3)$$

It results in 2×2×3=12 partial relations; the first 3 of them (**C**,**ID**), (**C**,**AU**), (**C**,**VR**) refer to common client identification/authorization/authentication methods; next three ones extend the **ID**, **AU**, **VR** notions into the sphere of info-resources management.

The last 6 members of product (3) define a local AI-aided cybersecurity model in the form of six independent tasks

$$\text{S-CDM}_{AI\text{-}CS} := \mathbf{(\,)}_{AI} \times [\mathbf{C}, \mathbf{R}] \times [\mathbf{ID}, \mathbf{AU}, \mathbf{VR}]. \quad (4)$$

The Cartesian-product member [**( )$_{AI}$**, **C**, **VR**] in (4) defines a cluster "AI-aided methods and operational tools for client verification (authentication)", which can be taken as a next step of researches.

Consider a comprehensive AI-to-cybersecurity survey [27] (2023) with 247 references. In includes 6 "identity-authentication" AI-related items: "Bio-signal classification for human identification based on convolutional neural networks"; "Improving the security and QoE in mobile devices through an intelligent and adaptive continuous authentication system"; "Securing smart offices through an intelligent and multi-device continuous authentication system"; "An approach to detect user behavior anomalies within identity federations"; "Web user authentication using chosen word keystroke dynamics"; "Keystroke identifier using fuzzy logic to increase password security".

Thus, it is possible to identify a compact area of knowledge and related publications for systemic research as part of a larger problem. Herewith, specific relevant facts can be fixed, e.g.: human identification systems use signal acquisition, signal pre-processing, and feature extraction/classification extracted from the images based on convolutional neural networks (ref. 90); permanent authentication of mobile devices owner provides user profile generation and real-time comparison of the current mobile usage with typical user's behavior using by ML techniques (ref. 91).

6 DISCUSSION

The 20th century evidences formation a new fundamental vision of things and problems around us. Many challenges require a deep insight on complex objects study with a large number of components, for which the constituent's issues are accompanied by their interaction's concerns.

An efficient instrument of general system theory (GST) is hierarchical decomposition a given large object of study into a set of interconnected partial tasks. But, implementation of this instrument is somehow a creativity art rather than a trivial engineering task. In particular, a difficult task is relevant definition of interconnected semantic classes of things with respect to given problem study.

A critical problem today is Internet of things systems and networks privacy. In spite of significant progress in both wired and wireless IoT-technologies, new tasks and challenges emerge, e.g. in the context of advanced not clear predicted artificial intelligence capabilities.

This work focuses the IoT privacy object of study as a complex cybersecurity problem. As a first approach to this problem solution, a GST-decomposition formalism proposed, that converts down the overall cybersecurity object into a set of 24 interacting partial tasks of less complexity. The objects components are clients, resources and agents of the information market, along with network communication means.

Within the scope of this work, an original cyber security context-defined model S-CDM of open systems interaction constructed on the base of J. Neumann ternary classification and A. Uemov system triad for the IoT privacy issues study.

The S-CDM-model is shaped in 3-layer hierarchical graph. The S-CDM1 layer displays the cybersecurity problem as a set of relationships between the clients, resources and agents.

The S-CDM2 layer adds network technologies impact on the relations between the key market-players.

The S-CDM3 layer includes the “degree of trust” factor in relationships between the key market-players.

The introduced S-CDM model provides decomposition of a complex cybersecurity problem to a number of less complex and easy-handled partial tasks.

7 CONCLUSIONS

This article addresses the problem of cybersecurity within the IoT architecture, focusing on privacy protection amidst the challenges of digital transformation and rapid advancements in artificial intelligence. The analysis revealed that IoT is characterized by a complex structure requiring a systematic approach to solve issues related to data protection, identification, authentication, and authorization.

The primary method proposed involves decomposing a complex problem into a number of interconnected sub-problems on the base of general systems theory. A novel context-defined model of open system interaction S-CDM was developed to structure the IoT cybersecurity problem into less complex tasks. This model provides a foundation for building localized and AI-enhanced models aimed at the identification, verification, and authorization of clients and resources.

The research also demonstrated that artificial intelligence plays a pivotal role in securing IoT through mechanisms such as continuous authentication, biometric signal classification, and anomaly detection in behavior. Special emphasis was placed on integrating IoT into industrial systems (IIoT) within the framework of Industry 4.0.

The results of the work intend to contribute general system researches in the sphere of network system modelling and IoT privacy.

ACKNOWLEDGMENTS

We acknowledge support by the German Research Foundation (Deutsche Forschungsgemeinschaft, DFG) and the Open Access Publishing Fund of Anhalt University of Applied Sciences.

REFERENCES

[1] A. Dennis et al. “System analysis and design”, 5th ed., John Wiley & Sons, 2012, 563 p. [Online]. Available: https://www.google.com/search?client=safari&rls=en&q=Dennis+A.+Wixom+B.H.+System+Analysis+and+Design+5+Ed++pdf&ie=UTF-8&oe=UTF-8.

[2] A.E. Kononuk "Systemology. General System Theory", Book 1. Basics, Kiev, 2014, 568 p. [Online]. Available: https://z-lib.io/book/16404592f.

[3] A. Dennis et al., System Analysis and Design, 5th ed., John Wiley & Sons, 2012, 563 p. [Online]. Available: https://www.google.com/search?client=safari&rls=en&q=Dennis+A.+Wixom+B.H.+System+Analysis+and+Design+5+Ed++pdf&ie=UTF-8&oe=UTF-8.

[4] A. E. Kononuk, Systemology. General System Theory, Book 1. Basics, Kiev, 2014, 568 p. [Online]. Available: https://z-lib.io/book/16404592f.

[5] T. Cody et al., “Motivating a Systems Theory of AI,” ResearchGate Special Feature, vol. 23, no. 1, pp. 37-40, 2020. [Online]. Available: https://www.researchgate.net/publication/340652980_Motivating_a_Systems_Theory_of_AI.

[6] K. Lang et al., “A systems theory-based conceptual framework for holistic digital transformation,” 2021, 24 p. [Online]. Available: https://www.researchgate.net/publication/352020735_A_systems_theory-based_conceptual_framework_for_holistic_digital_transformation.

[7] Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, President’s Council of Advisors on Science and Technology, 2023, 36 p. [Online]. Available: https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

[8] M. Abomhara and M. Koien, “Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks,” Journal of Cyber Security, vol. 4, pp. 65–88, 2015. [Online]. Available: https://www.researchgate.net/publication/349642687_Cyber_Security_and_the_Internet_of_Things_Vulnerabilities_Threats_Intruders_and_Attacks.

[9] M-Bus und M-Bus Wireless Grundlagen. [Online]. Available: https://www.wachendorff-prozesstechnik.de/technologie/feldbus/m-bus/.

[10] H. Ziegler, Serial BUS Systems. [Online]. Available: https://m-bus.com/assets/downloads/MBDOC48.PDF.

[11] S. Payne, “Zigbee Technology: Everything You Need to Know for IoT,” 2023. [Online]. Available: https://www.telit.com/blog/zigbee-iot-guide/.

[12] ZigBee PRO/2007 Layer PICS and Stack Profiles, Rev. 08, 2018. [Online]. Available: https://infocenter.nordicsemi.com/pdf/Zigbee_PRO_Layer_PICS_and_Stack_Profile_8.pdf.

[13] “Y.2060: Overview of the Internet of Things,” 2012. [Online]. Available: https://www.itu.int/rec/T-REC-Y.2060-201206-I.

[14] “IoT Reference Model Introduced at IoT World Forum 2014.” [Online]. Available: https://ytd2525.wordpress.com/2014/10/22/iot-reference-model-introduced-at-iot-world-forum-2014/.

[15] "IoT World Forum Reference Model," 2014. [Online]. Available: https://www.researchgate.net/figure/IoT-World-Forum-Reference-Model_fig2_323525875.

[16] "What is Industry 4.0?". [Online]. Available: https://www.ibm.com/topics/industry-4-0/.

[17] J. Voas, Networks of Things, NIST Special Publication 800-183, 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-183.pdf.

[18] "IIoT Explained: Examples, Technologies, Benefits and Challenges." [Online]. Available: https://www.emqx.com/en/blog/iiot-explained-examples-technologies-benefits-and-challenges.

[19] "Dotdot was a huge hit at CES 2017." [Online]. Available: https://www.symmetryelectronics.com/blog/dotdot-was-a-huge-hit-at-ces-2017/.

[20] "What is Dotdot?". [Online]. Available: https://en.dsr-corporation.com/news/what-is-dotdot.

[21] IEEE 802.15.4 Standard for Low-Rate Wireless Networks, 2020. [Online]. Available: https://store.accuristech.com/standards/ieee-802-15-4-2020.

[22] R. Joshi et al., The Industrial Internet of Things Connectivity Framework, 2022. [Online]. Available: https://www.iiconsortium.org/wp-content/uploads/sites/2/2022/06/IIoT-Connectivity-Framework-2022-06-08.pdf.

[23] C. Baudoin et al., "Global Industry Standards for Industrial IoT," 2022. [Online]. Available: https://www.iiconsortium.org/pdf/IIC_Global_Standards_Strategy_Whitepaper.pdf.

[24] "EMQX Overview." [Online]. Available: https://docs.emqx.com/en/emqx/latest/.

[25] M. A. Razzaq et al., "Security Issues in the Internet of Things (IoT): A Comprehensive Study," International Journal of Advanced Computer Science and Applications, vol. 8, no. 6, pp. 383-388, 2017.

[26] "Zigbee Security 101. Architecture And Security Issues," 2023. [Online]. Available: https://payatu.com/blog/zigbee-security-101-architecture-and-security-issues/.

[27] The Industrial Internet Reference Architecture, 2022. [Online]. Available: https://www.iiconsortium.org/wp-content/uploads/sites/2/2022/11/IIRA-v1.10.pdf.

[28] Industrial Internet of Things. Volume G4: Security Framework, 2016. [Online]. Available: https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf.

[29] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," Elsevier, Information Fusion, vol. 97, 2023.