МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

МІНІСТЕРСТВО ОСВІТИ ІРАКУ
AL-RAFIDAIN UNIVERSITY COLLEGE

МІНІСТЕРСТВО ОСВІТИ І НАУКИ ПОЛЬЩІ
УНІВЕРСИТЕТ КОМІСІЇ НАРОДНОЇ ОСВІТИ В КРАКОВІ

III Міжнародна науково-практична конференція “Новітні технологічні тенденції інтелектуальної індустрії та Інтернету речей”

«TTSIIT»

25-26 січень 2024р.
Україна-Ірак-Польща

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
KYIV NATIONAL UNIVERSITY OF CONSTRUCTION AND ARCHITECTURE

MINISTRY OF EDUCATION OF IRAQ
AL-RAFIDAIN UNIVERSITY COLLEGE

MINISTRY OF EDUCATION AND SCIENCE OF POLAND
UNIVERSITY OF THE NATIONAL EDUCATION COMMISSION OF KRAKOW

The 3rd International Conference on Emerging Technology Trends on the Smart Industry and the Internet of Thing

«TTSIIT»

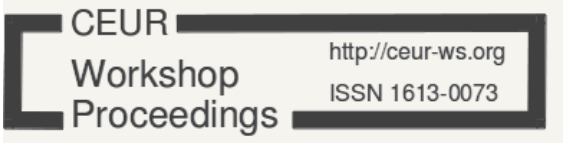
January 25-26, 2024
Ukraine-Iraq-Poland

РЕДАКЦІЙНА КОЛЕГІЯ:

Конференція проведена за організаційної, інформаційної та технічної підтримки кафедри кібербезпеки та комп'ютерної інженерії КНУБА (завідувач кафедри д.т.н., проф. Хлапонін Ю.І.)

Рекомендовано вченою радою Київського національного університету будівництва і архітектури. Протокол № 19 від 23.02.24 р.

Відібрані оргкомітетом доповіді після допрацювання опубліковані в виданні, яке індексується в наукометричній базі Scopus



Зміст

ВСТУПНЕ СЛОВО. INTRODUCTORY WORD

Петро Куліков

Професор, доктор економічних наук,
Ректор Київського національного університету будівництва і архітектури.
Почесний академік Національної академії педагогічних наук України,
Лауреат Державної премії України в галузі науки і техніки.
Заслужений працівник освіти України,
Президент Спілки ректорів закладів вищої освіти України,
Віце-президент Будівельної палати та Академії будівництва України

Шановні учасники конференції!

Між нашими Університетами підписані Меморандуми про співпрацю. І сьогодні ми маємо нагоду прийняти участь у спільному заході – конференції, яка організована ініціативними групами наших університетів.

Наш університет готує фахівців з будівельних та архітектурних спеціальностей, а також зацікавлений у підготовці фахівців з таких перспективних напрямків, які сьогодні будуть обговорюватися на конференції. Тема конференції на сьогоднішній день є дуже актуальною, тому що в будівництві впроваджуються нові технології, такі як “Розумний будинок”, “Розумне місто” та впроваджуються технології Інтернету речей при експлуатації житлових та промислових будівель. КНУБА має тісні партнерські зв’язки з будівельними компаніями та може запропонувати архітектурні та будівельні рішення та проекти житлових та промислових об’єктів.

Сподіваюсь, що робота конференції буде плідною, ми виступимо з доповідями та поділимося результатами своїх наукових досліджень.

Бажаю успіху!

DIGITAL TRANSFORMATION AND IoT IN EDUCATION AND SCIENCE OF UKRAINE IN THE CONTEXT OF EUROPEAN INTEGRATION

Tetiana KONRAD (PhD., associate professor, Institute of Technical Sciences)[1]
Henryk NOGA (Dr hab, professor, Director of the Institute of Technical Sciences)[1]
Svitlana KORNIENKO (Assistant)[2]

[1] *University of the National Education Commission, Krakow, Poland*
[2] *National Aviation University, department of Software Engineering, Kyiv, Ukraine*
[1] konrad.t_i1@ukr.net, [2] spkorn@ukr.net

Abstract

Abstract. The paper analyzes the current state and prospects of digital transformation and IoT technologies in education and science in Ukraine in the context of European integration. The implementation of the EU-Ukraine Agreement in these areas is analyzed. The main state initiatives and international projects within the framework of digitalization of higher education and science in Ukraine are considered. Prospects for the digital transformation of education and science in Ukraine for the implementation of strategic partnership with the EU countries are identified.

Keywords

Digitization, digital transformation, IoT, computer technologies, education, science, digital competence.

Relevance of research

The full-scale war in Ukraine has become a test and a shock for both Ukrainian society and the Ukrainian education and science system. In the context of the intensification of hostilities, an important issue is to ensure the continuous and high-quality functioning of Ukrainian educational and scientific institutions, further implementation and development of state educational initiatives, as well as compliance with the state's strategic course towards Ukraine's full membership in the European Union (EU). Among the approved strategic and operational goals for the development of higher education in Ukraine [1] are the following: integration of the Ukrainian education and science system into the European Higher Education Area (EHEA) and the world education area; creation and implementation of the industry of innovative technologies and distance learning tools; digitalization of all processes in the higher education system, as well as ensuring the quality and accessibility of higher education. Thus, it is advisable to analyze the current state of the digital transformation of education and science in Ukraine, which will contribute to the post-war recovery of the sector and the implementation of the strategic partnership with the EU.

The purpose of the article consists the analysis of the current state and prospects of the digital transformation and IoT technologies sn education and science in Ukraine

for the need to speed up the process of integration of the system of education and science into the European space of higher education within the framework of Ukraine's strategic partnership with EU countries.

Presentation of the main research material

Digital transformation (digitalization) is the transformation of existing analog (sometimes electronic) products, processes, and business models of an organization based on the effective use of digital technologies [2]. According to the analytical reports of the Davos Economic Forum, the most common modern digital technologies are the Internet of Things, robotization and cyber systems, artificial intelligence, big data, paperless technologies, additive technologies (3D printing), cloud and fog computing, unmanned and mobile technologies, biometric technologies, quantum technologies, identification technologies, and blockchain. This list is not exhaustive and can be supplemented.

The basic principles of digitization include [2]:

1. Equal access to services, information and knowledge provided on the basis of information, communication and digital technologies.
2. Creating advantages in various areas of everyday life, improving the quality of services, including educational ones.
3. Increasing efficiency, productivity and competitiveness through the use of digital technologies.
4. Promoting the development of the information society and mass media.
5. Focusing on international, European and regional cooperation with the aim of Ukraine's integration into the EU and access to the European and global markets.
6. Increasing the level of trust and security.
7. Removing legislative barriers, launching national-level digital transformation projects and attracting appropriate investments, and stimulating the development of digital infrastructures.

Digital transformation in education and science is a comprehensive work on building an ecosystem of digital solutions in education and science, including the creation of a secure electronic educational environment, provision of the necessary digital infrastructure for educational and scientific institutions, raising the level of digital competence, digital transformation of processes and services, as well as automation of data collection and analysis [3].

IoT in education is the use of digital and Internet smart devices for students and teachers in educational institutions. Modern educational platforms adapt e-books, smart boards, voice control systems, tablets and smartphones with educational programs, virtual libraries, professional training and resource sharing tools.

State initiatives within the scope of digital transformation and IoT in the higher education in Ukraine are the following [3]:

Submission of applications by entrants in electronic form and corresponding accounting of these applications by the Ministry of Education and Science of Ukraine.

Creation of a new module to display the admission, as well as the electronic office of the entrants.

Creation of a new module for entering information about foreign students of preparatory departments into the Unified State Electronic Database on Education (EDEBO).

Implementation of registration of diplomas of Doctor of Philosophy / Arts, and Doctor of Science with the assignment of a registration number in the EDEBO by higher education institutions and scientific institutions.

Implementation of functions for the formation of European-style applications.

Electronic licensing in the field of education (e-licensing).

Implementation in EDEBO of the display of the license examination conducted by the expert commission of the licensing body, the generation of verification reports of the licensee's compliance.

EDEBO data exchange with external systems. Expanding the interaction of the «EDBO» with state automated systems and information resources, including by integrating additional services and clients into the EDEBO (with the help of an application software interface or tools of the electronic interaction system of state electronic information resources «Trembita»).

Monitoring the employment of graduates. Creation and modernization of a single electronic system for monitoring the employment of graduates to inform stakeholders about the career trajectories of graduates and make management decisions.

State initiatives of digital transformation and IoT in the field of science of Ukraine [3]:

Register of Ukrainian research infrastructures (Register of infrastructures). Creation and full functioning of a digital system of unified information profiles of Ukrainian research infrastructures (including existing equipment and specialists who work directly on it).

Open Ukrainian scientific citation index. Improvement of the Open Ukrainian scientific citation index by ensuring the use of a wide range of databases on the publications of Ukrainian scientists.

E-documents in Diya. Work continues the implementation of electronic documents about education on the portal and in the «Diya» mobile application. Currently, a draft resolution has already been developed for the regulatory regulation of the display in electronic form of information contained in documents about basic secondary, full general secondary, professional (vocational-technical), vocational pre-university, and higher education employing the Unified state web portal of electronic services using a mobile application «Diya».

Also, students, applicants, teachers, and educational managers have the opportunity to use 46 services that help to receive educational services remotely or online.

The Association Agreement between Ukraine and the European Union, in particular Title V. Economic and Sectoral Cooperation [4] defines Ukraine's commitments in the

fields of science and technology, as well as education, training and youth to implement strategic sectoral partnerships.

Cooperation between Ukraine and the EU in the field of science and technology provides for: exchange of information on policy in the field of science and technology; joint implementation of scientific programs and research activities; joint study of activities aimed at promoting scientific progress, technology transfer and know-how; activation of regional and other international cooperation.

Cooperation between Ukraine and the EU in the field of education, training and youth provides for: reform and modernization of the higher education system; expansion of opportunities of higher educational institutions; activation of mobility of students and teachers; simplifying access to higher education; carrying out activities aimed at intensifying the exchange of information, practice and experience, to encourage closer cooperation in the field of vocational education and training.

The progress of the implementation of the Association Agreement between Ukraine and the EU is carried out on an ongoing basis by the information and analytical system (IAS) for monitoring the implementation of the Association Agreement «Pulse of the Agreement», the system is publicly available [5]. The interface of the information and analytical system graphically displays the monitoring data of the implementation of the plan of measures for the implementation of the Agreement and the progress of implementation.

The overall progress in the implementation of the tasks under the section "Education, Training and Youth" is currently 94% of the total amount of tasks; under the section "Science, Technology and Innovation, Space" - 65%.

For the full implementation of the agreement on association and integration of education and science of Ukraine into the European Higher Education Area, the following tasks need to be addressed: information exchange; improving the quality and accessibility of higher education, and intensifying innovation; technology transfer.

Continuing the digitalization and implementation IoT in education and science will contribute to solving these problems.

Conclusions

The analysis of the state of digital transformation and IoE in education and science in Ukraine has shown a high level of progress in the implementation of the Association Agreement between Ukraine and the European Union.

The active implementation of government digital initiatives and continued international cooperation will contribute the development of Ukraine's information society, education and science sectors, strategic partnership with the EU and the integration of education and science of Ukraine into the European Higher Education Area.

References

[1] Higher education development strategy in Ukraine for 2021–2031 (2020), Ministry of Education and Science of Ukraine, Official Website Publ. https://mon.gov.ua/storage/app/media/rizne/2020/09/25/rozvitku-vishchoi-osviti-v-ukraini-02-10-2020.pdf Accessed 10 Oct 2023.
[2] UKRAINE 2030E – A COUNTRY WITH A DEVELOPED DIGITAL ECONOMY, Ukrainian Institute of the Future, Official Website Publ. https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html. Accessed 10 Oct 2023.
[3] DIGITAL TRANSFORMATION OF EDUCATION AND SCIENCE, Ministry of Education and Science of Ukraine Publ. https://mon.gov.ua/ua/tag/cifrova-transformaciya-osviti-ta-nauki. Accessed 10 Oct 2023.
[4] Text of the Agreement (2017), EUROPEAN INTEGRATION PORTAL, Official Website Publ. https://eu-ua.kmu.gov.ua/tekst-uhody-pro-asotsiatsiiu. Accessed 10 Oct 2023.
[5] Monitoring the implementation of the plan of measures for the implementation of the Agreement, Pulse of the Agreement, Official Website Publ. https://pulse.kmu.gov.ua/. Accessed 10 Oct 2023.

ARCHITECTURE OF A MULTI-AGENT INFORMATION-ANALYTICAL SYSTEM FOR PREDICTING LOSSES UPON THE MATERIALIZATION OF THREATS TO A BANK'S INFORMATION SECURITY

Kateryna KRASOVSKA (PhD, Senior Business Analyst, SoftServe Poland)

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
katerina.krasovska@gmail.com

Abstract

This paper presents the architecture of a multi-agent information-analytical system designed to predict losses following the materialization of threats to a bank's information security. Integrating diverse mathematical models, including self-organizing Kohonen maps, k-nearest neighbors, and generalized regression networks, this system enhances the effectiveness of threat analysis and loss prediction. The findings demonstrate the system's potential to not only improve current risk management strategies in banks but also to serve as a foundation for further development of predictive software tools including application of proposed IAS to other subject areas.

Key words

Multi-agent information-analytical system, Agent-oriented approach, Loss prediction, Bank information security, Neural networks and machine learning

Introduction

A key element in the operation of banks and the banking system as a whole is the effective resolution of issues related to ensuring information security, as well as the assessment of consequences and analysis of mechanisms for the materialization of threats to information security of the bank. The analysis of consequences and efficient evaluation of losses upon the materialization of threats enable the refinement of existing systems for countering threats and, additionally, permit the use of this experience for risk assessment and determination of the acceptability level of various threats. This, in turn, increases the flexibility of banking processes and enhances the competitive capability of financial institutions. The results obtained from threat analysis and loss estimations provide a basis for forecasting the materialization of threats, anticipated losses, and the creation of mitigation strategies upon the realization of various types of threats.

For an effective analysis of threats and estimation of expected losses, diverse technologies must be utilized, providing tools to solve the problems at hand. For instance, the study [1] suggests the use of scenario-based approach and analysis of expert assessments to determine expected losses from the realization of various threats to a bank's information system. Furthermore, many researchers prefer the use of neural networks and machine learning for detecting and countering threats. The authors of

study [2] propose an algorithm for identifying fraudulent activities with bank cards using technologies such as Kohonen's self-organizing maps (SOM). In study [3], methods like Random Forest, k-nearest neighbors (KNN), and Support-Vector Machine (SVM) are examined. Study [4] confirms that neural networks and machine learning are promising tools with broad applications in various spheres of risk management for banks and financial institutions.

The application of multi-agent technologies for the analysis and detection of threats in banks and banking systems deserves special mention, offering possibilities for enhancing the expert approach and approaches involving neural networks and machine learning. For example, in studies [5] and [6], agents are used to identify fraudulent activities, and in the research [7], the development of an automated decision support system (DSS) is proposed. This system is capable of self-learning and autonomous operation and ensures cooperation with both the human expert and between internal or external components of the system. These principles are implemented through the development of a multi-agent system that resolves the stated problem.

Therefore, the aim of this work is to determine the architecture of the proposed multi-agent system in [7].

Main part

The work proposes the application of an agent-oriented approach to the design of multi-agent systems, which includes the construction of the following models: an agent model, an organizational model of the multi-agent system, and a model for agent interactions. The design process consists of the following steps:

1. Defining roles within the system and their interrelations, that is, constructing a **role model**.
2. Constructing an **agent model**, specifically defining agents in the system based on the role model.
3. Constructing a **service model**, namely the functions that the agents perform.
4. Constructing a **model of contracts**, i.e., the connections between agents.

In the study [1], the steps for the scenario of assessing expected losses upon the materialization of threats to a bank's information security are defined as follows:

1. Assessment by experts focus group of the probability of possible levels of loss for each criterion $f_j \in F$ upon the materialization of a threat to the bank's information assets.
2. Evaluation of the expected values of criterion indicators of loss.
3. Generalized assessment of the group of experts of the expected criterion indicators of loss.

To automate the proposed scenario, the following architecture of the multi-agent system is used (see Fig. 1).

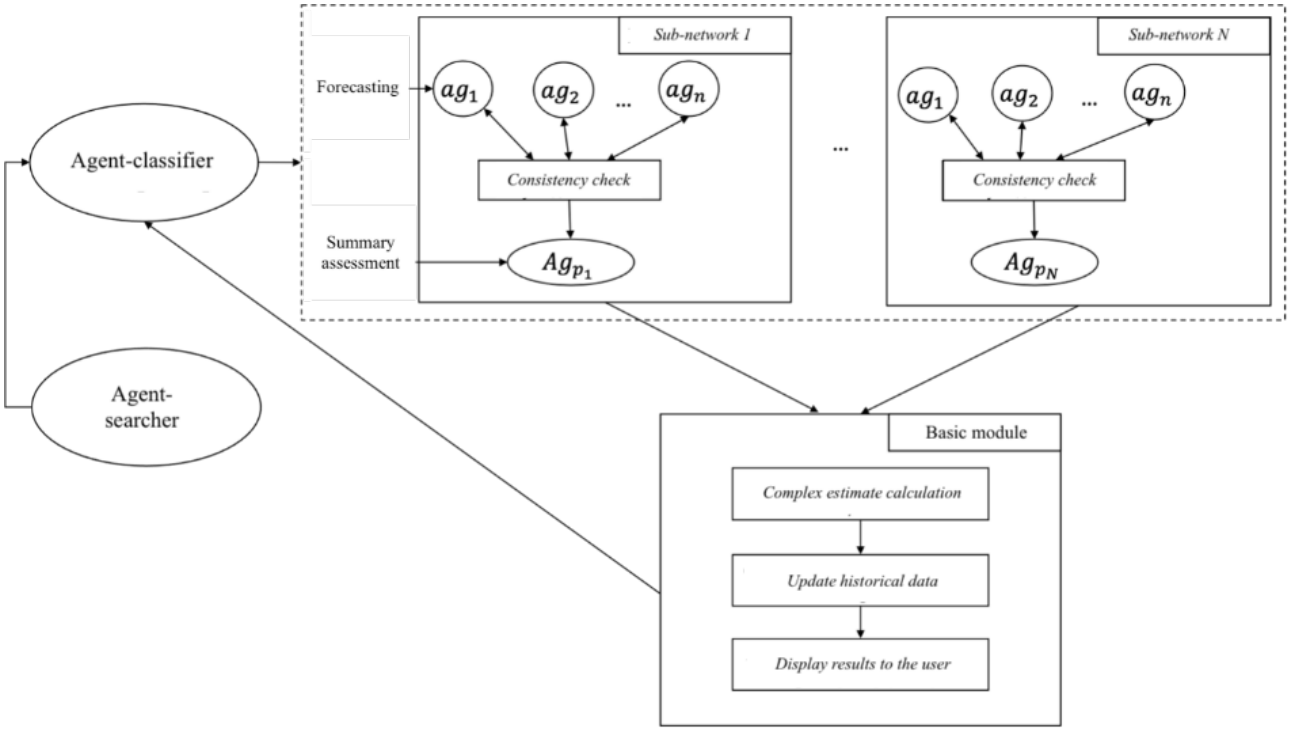


Fig. 1. Multi-agent system architecture

It is also important to note that for the optimization of the proposed scenario, preliminary data preparation is necessary, including information regarding previous instances of threats materialization to the bank's information security. The available information should be grouped into certain classes by types of emerging threats.

For existing instances of threat materialization, the actual classes of losses incurred upon the realization of a given threat should be identified. Moreover, as information regarding the materialization of threats, threat classes, and losses is updated from time to time, a tool for collecting and consolidating information is necessary. For this purpose, the use of a **agent-searcher** is proposed. This agent receives data about the location of necessary information at its input, namely databases containing available information about instances of threat materialization and threat classes, and provides consolidated information about the materialization of threats from various data sources at its output.

The automation of the approach proposed in [1] is impossible without the automatic classification of a new instance of threat materialization into a certain type of threat. For this purpose, the use of a classifier agent built on the basis of Kohonen's self-organizing maps is proposed. Utilizing the training set of existing instances of threat materialization, which is normalized and updated by the agent-searcher, the **agent-classifier** forms profiles for each type of threat and, upon the occurrence of a new instance of threat materialization, assigns it to a particular threat profile-cluster.

Following the steps of the scenario, it is necessary to determine the expected level of loss upon the materialization of a threat for each criterion indicator $f_j \in F$. For the computation of expected loss values, the use of sets of sub-networks of different types

of agents is proposed. Suppose there exists $p_i \in P, i = \overline{1,N}$ agent sub-networks. In each sub-network p_i, t agents operate: $p_i = \{ag_1, ag_2 \dots ag_t\}$. It is important to note that the sub-networks p_i are isolated from each other. After the agent-classifier has determined the threat realization profile-cluster, information regarding the expected losses for each case from the given cluster is transmitted to the input of the agent sub-networks. This information is divided into parts depending on the number of agents set during the system's initialization. Each agent conducts an assessment regarding the possible class of expected losses upon the realization of a new instance of the given type of threat. As mentioned above, the use of different types of agents is proposed in order to enhance the quality of the evaluation, namely:

- An agent based on the k-nearest neighbors algorithm;
- An agent based on a generalized regression network.

Thus, each agent ag_k from the sub-network $p_i = \{ag_1, ag_2 \dots ag_t\}$, where $p_i \in P, i = \overline{1,N},\ k = \overline{1,t}$, acts as a **forecasting agent**, which receives information about a new instance of threat materialization as its input, and using information about the loss levels of a certain threat profile, issues a probable level of loss for the new case as its output.

The next step is to perform a convolution of the obtained estimates. For this purpose, in each sub-network, a **convolution agent** $Ag_{p_i} \in P$, $i = \overline{1,N}$ is used, which generalizes the assessments obtained from the agents $ag_i \in p_i$ for each criteria f_j. The convolution agent transmits the data to the **basic module**, which also acts as an agent that performs the calculation of the generalized assessments of expected criterion indicators. The obtained results are available for review by the Decision Maker (DM) in the user interface of the system. The basic module also performs updates of historical data and transmits information to the classifier agent for storage.

Conclusions

The proposed architecture of the multi-agent information-analytical system (IAS) allows automated assessment based on developed diverse mathematical models and methods for predicting losses upon the materialization of threats to the bank's information security. For the preliminary processing of data on instances of information system (IS) threats at the bank and subsequent forecasting of expected levels of losses, self-organizing Kohonen maps are used, and the k-nearest neighbors algorithm and generalized regression network are applied for assessment. The automation of the assessment process and prediction of expected losses will enhance the efficiency of the logical-mathematical apparatus for expert assessment developed in [1]. The developed logical-mathematical apparatus and the designed architecture of the multi-agent IAS create a foundation for the development and implementation of corresponding software that can be applied in practice. Furthermore, there are opportunities for further development and optimization of the developed models, methods, and algorithms, for instance, through the use of other types of neural networks and conducting a comparative

assessment of algorithm efficiency, as well as the tuning and application of the developed models, methods, and algorithms in other subject areas.

References

[1] Izmailova, O., Krasovska, H., Krasovska, K., & Zaslavskyi, V. (2020). Assessing the Variety of Expected Losses upon the Materialisation of Threats to Banking Information. In "Information & Security: An International Journal," 45, 89-118. https://doi.org/10.11610/isij.450

[2] Zaslavsky, V., & Strizhak, A. (2006). Credit Card Fraud Detection Using Self Organizing Maps. In "International Journal Information & Security," 18, 48-63.

[3] Gill, M. A., Ahmad, N., Khan, M., Asghar, F., & Rasool, A. (2023). Cyber Attacks Detection through Machine Learning in Banking. In "Bulletin of Business and Economics," 12(2), 34-45. https://doi.org/10.5281/zenodo.8310116

[4] Leo, M., Sharma, S., & Maddulety, K. (2019). Machine Learning in Banking Risk Management: A Literature Review. In "Risks," 7(1), 29. https://doi.org/10.3390/risks7010029

[5] Buoni, A. (2012). Fraud Detection in the Banking Sector: A Multi-Agent Approach. Dissertation, 181 pp. Retrieved from https://www.doria.fi/bitstream/handle/10024/84911/buoni_alessandro.pdf?sequence=1

[6] Amanze, B.C., Inyiama, H.C., & Onyesolu, M.O. (2018). On the Development of Credit Card Fraud Detection System Using MultiAgents. In "International Journal of Computer Sciences and Engineering," Vol.6(6), E-ISSN: 2347-2693.

[7] Izmailova, O.V., Krasovska, H.V., & Krasovska, K.K. (2022). Multiagentnyy pidkhid pry pobudovi stsenariyu otsinky ochikuvanykh zbytkiv pry realizatsiyi zahroz informatsiynoyi bezpeky banku. In Proceedings of The 1st International Conference on Emerging Technology Trends on the Smart Industry and the Internet of Things (pp. 43-45), January 19th–20th 2022.

SPACE INTERNET OF THINGS: OPPORTUNITIES AND CHALLENGES

[1] **John MAGILL** (M.Phil, Control Engineering and Operational Research)
[2] **Svitlana KONDAKOVA** (PhD, Associate Professor)

[1] *Cambridge University, Department of Engineering, Cambridge, England*
[2] *Kyiv National University of Contracture and Architecture, Faculty of Automation and Information Technologies, Department of Cyber Security and Computer Engineering, Kyiv, Ukraine*
[1] john.magill@cantab.net , [2] kondakova.sv@knuba.edu.ua

Abstract
This paper introduces the topic of "Space Internet of Things" and surveys some of the literature. It considers the opportunities and the challenges of Space IoT.

Introduction

It is often said that as the internet matures, and becomes more a part of our everyday lives, the original "Internet of People" is becoming the "Internet of Things". The internet of things can be regarded as the enabler of "smart" in the context of smart homes, smart heating, smart fridges etc.

Internet of Things devices usually rely on cellular networks, which can lead to problems in areas not well served by such networks. Satellite communication offer a means to overcome some of these limitations. This paper will consider two aspects:

* Use of Space (specifically satellite communications) to enhance Terrestrial IoT networks

* Extension of Terrestrial IoT to Space applications

This is a new and developing area, in which even the terminology has not been settled, or the boundaries defined, but the following terms can be found in the literature:

“Space Internet of Things” ref [1]

“Internet of Space Things” ref [2]

“Internet of Things in Space” ref [3]

"Satellite Internet of Things" refs [4] and [5]

Doubtless a proper taxonomy, with suitable Venn diagrams, will be developed in due course.

The figure below, from ref [3] usefully depicts the complete IoT communications "ecosystem" including how space fits in to complete the picture:

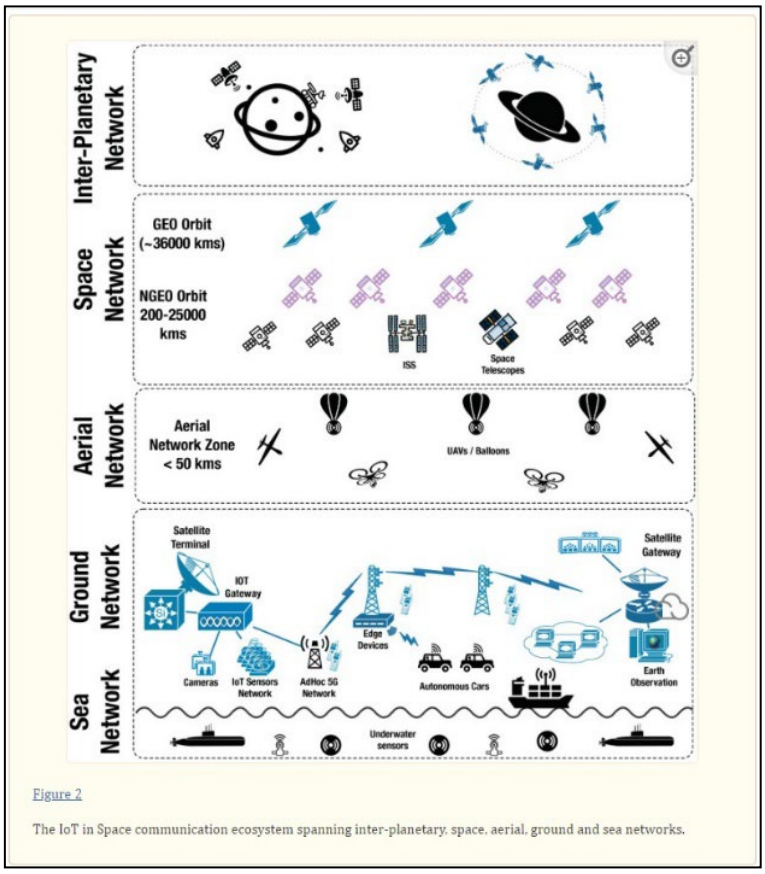


Fig 1. Complete IoT communications "ecosystem"

Benefits of Satellite Communications

Satellite communications can offer:

* increased **Capacity -** in terms of bandwidth

* increased **Coverage** - Especially over areas not currently well served by fixed line or wireless services. Typically these would be poorer, more remote areas, which often have needs to monitor:

Crops, livestock, natural disasters such as floods, earthquakes etc;

BARTSCH ref [4], identifies the following IoT-enabled services that would be likely to benefit from satellite links:

* Marine telematics
* Smart agriculture
* Oil and gas
* Mining
* Construction
* Transportation

Trends in Satellite Communications:

Trends in satellite communications in recent decades have tended to be away from large, expensive, highly reliable communications satellites in geostationary orbit

(GEO) and towards large constellations of smaller satellites in low earth orbit (LEO). The advantages of the former include the fact that only 3 such satellites are required for coverage of most of the earth (excepting high latitudes), and that as the satellites appear to be "stationary" in the sky, there are fewer issues with tracking in angle or in Doppler. Against these advantages are the need for high transmitter powers, high reliability, and latency issues resulting from the inevitable ~80,000km round trip time, plus any delays associated with signal processing. Smaller satellites in lower orbits require less transmitter power, but large constellations are required to maintain coverage, while users may need to track the satellites as they move across the sky both in angle and Doppler, and "hand over" from one satellite to another as satellites rise and set.

Despite lower transmitter power requirements, small satellites always face the challenge of generating sufficient power to operate successfully. Reliability of such satellites may be lower, but expected lifetimes are shorter as there will be a steady cycle of launch, replacement and decommissioning of old satellites. But since many satellites are needed to provide coverage, shorter lifetimes can be tolerated given sufficient redundancy and or replacement launches.

Satellites for IoT

Many of these issues associated with LEO satellites to provide IoT are common to other applications, such as for mobile communications, so the use of such constellations for space IoT need not introduce any further problems. Possibly **latency** issues might be significant, depending on the application – think self-driving cars - while other IoT applications may be relaxed on latency requirements

Space IoT applications

KUA ref [3] identifies the following emerging or potential "in space" applications:

1 Smart Architecture and Construction in Space, incl use of Robots;
2 Data Centres in Space and Data Management Services for In-Space Operations
3 Robots in Space
4 Connected Automated Space Vehicles
5 Networked Wearables and Apps in Space
6 Space Situational Awareness, Dealing with Space Debris and Space Traffic Management
7 Colonising Planets (- lest we find ourselves limited in our ambitions!)

These, along with topics more down to earth are well depicted in a "Taxonomy" diagram from ref[3]:

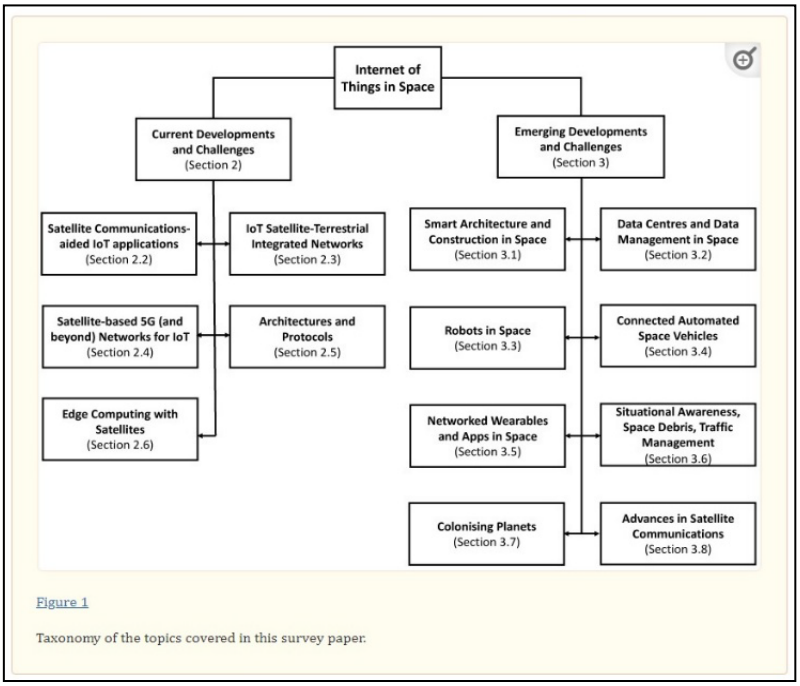


Fig 2. "Taxonomy" diagram

Conclusions

Space IoT is an emerging field that offers benefits both to terrestrial IoT applications and also to extend the scope of IoT into ever remoter and more distant regions.

References

[1] NARAYANA, S. TU Delft "Space Internet of Things (Space-IoT)" https://research.tudelft.nl/en/publications/space-internet-of-things-space-iot
[2] IoT MARKETING: "Internet of Space Things: Extending IoT Applications in Space" https://iotmktg.com/internet-of-space-things-extending-iot-applications-in-space/
[3] KUA, J. et al: "Internet of Things in Space: A Review of Opportunities and Challenges from Satellite-Aided Computing to Digitally-Enhanced Space Living" https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8662413/
[4] BARTSCH, M. "What Is Satellite IoT? Closing Gaps in Global Connectivity" https://www.emnify.com/iot-glossary/satellite-iot
[5] INMARSAT: "Satellite IoT: the future of networking" https://www.inmarsat.com/en/insights/corporate/2023/satellite-iot-the-future-of-networking.html

THE ROLE OF ARTIFICIAL INTELLIGENCE IN VERIFYING THE CREDIBILITY OF INFORMATION ON THE INTERNET

Silvia MOMCHEVA (Bachelor, fourth-year student)

University of Economics, Faculty of Informatics, Varna, Bulgaria
silvia.momcheva@ue-varna.bg

Abstract
Technological solutions based on artificial intelligence (AI) are a powerful tool for verifying the accuracy of information on the internet. They help review vast amounts of data and perform complex analyses. AI can use various techniques for text analysis, such as machine learning and neural networks, to build models that show whether a given text is false or not.

Introduction

With the development of technology and the internet, access to information is easier and faster than ever. We can search for any topic, watch videos, listen to audio recordings, communicate with people from all over the world. The internet is full of information that can be easily published and shared without verifying its accuracy. This sometimes leads to the spread of false or misleading information, which can harm people, society, and business.

The goal of the report is to show how AI is used to determine the reliability of sources of information, the accuracy of facts, and their precision, as well as to reveal the possibilities of artificial intelligence for automating the process of verifying the accuracy of information. The study can be useful for media organizations, social networks, online stores, and other online platforms that need to control the quality of published information.

Traditional methods and technologies for verifying the credibility of information on the internet

1. Source verification

Who is the author of the information, where is it published and who maintains it. If the source is authoritative, such as a university, government organization, or well-known newspaper, it is likely to be more reliable. A participant, observer, or event analyst is verified as the author. Is he affiliated with a political party or corporation and whose interests does he protect? [1][2]

2. Fact check

It is checked whether the information is confirmed by other sources. If no other sources can be found that corroborate the facts, then it is more likely that there is a problem with the credibility of the information.

3. Search engines

Search engines such as Google, Bing or Yahoo are used to search for additional information on the topic. It is checked whether there are sources that support the information or there are those that refute it.

4. Date check

The date of publication of the information is checked. If the information is very old, it may be outdated or already changed.

5. Language assessment

The language and style of the information is checked. If it is written with errors, absurdities or is biased in a certain direction, then this may be an indication of lack of credibility.

6. Compare images

Images are checked to see if the photo is actually related to the topic and when it was first posted. A search with the Google or TinEye tool can be used.

7. Validating the URL

The URL of the page is checked - does it look strange or unfamiliar, does it have a free domain like .ml, .ga, does it have a lot of ads, etc. A visual assessment of the overall design of the site is also done.

8. Auxiliary verification sites

- Domain history check https://completedns.com/dns-history/
- Goes back in time and checked for suspiciously deleted information https://archive.org/
- Checked for previous abuses https://mediascan.gadjokov.com/ https://www.mywot.com/
- The site code is checked for identifiers if the site owner has other sites and what they are. https://spyonweb.com/
- Author verified – info, links, photos, social networks used https://webmii.com/

All this checking is, of course, slow and laborious. Errors and inaccuracies can always occur. Therefore, more and more people are turning to artificial intelligence for help, which in minutes can do a job that takes half a day of searching with the old methods.

The Potential of AI in Verifying the Credibility of Information on the Internet

1. Natural language processing (NLP) is the ability of a computer program to understand human language as it is spoken and written -- referred to as natural language. It is a component of artificial intelligence (AI). [5]

2. Machine Learning (ML): ML is a type of AI that allows computers to learn from data and improve their performance over time. [4]

3. Natural Language Generation (NLG): NLG is an AI technology that allows

4. Knowledge Graphs: Knowledge graphs are a way of representing knowledge in a structured format that can be easily analyzed by computers. [3]

5. Sentiment Analysis: Sentiment analysis is an AI technology that can be used to analyze the tone and emotion of a piece of content.

These are just a few examples of the AI technologies that can be used to verify the credibility of information on the internet. By combining these technologies with human expertise, it is possible to create more accurate and reliable systems for fact-checking and information verification.

Examples of successful applications of AI in verifying the credibility of information on the internet. [6]

1. Factinsect

https://factinsect.com/ uses AI to check the credibility of content. The fully automated tool compares text content with information from selected, trustworthy sources.

2. Vera.ai

DW is a partner in the vera.ai (Verification Assisted by Artificial Intelligence) project - https://www.veraai.eu/home. One of the project's aims is to build reliable AI solutions to identify disinformation.

DW is involved in three technological tasks, assisting respective task leaders: multilingual credibility assessment and evidence retrieval, audiovisual content analysis and multimodal deepfake and manipulation analysis.

3. The Factual

The Factual – https://www.thefactual.com/index.html provides a newsletter, app, Chrome extension, and website to users who want to be informed about the credibility of specific stories. The Factual is powered by an algorithm which rates the credibility of more than 10,000 news stories each day. Factors it considers include a site’s sourcing history, the author’s track record, and the diversity of sources in a news article.

4. Check by Meedan

Check is a fact-checking tool from technology non-profit Meedan - https://meedan.com/check. In 2019, Meedan launched a fact-checking project in combination with WhatsApp and Facebook using Check. The Check Platform enabled the open-source collection of tips through WhatsApp regarding misinformation in Africa, India, and Brazil.

5. Logically

Founded in 2017, Logically is a free mobile app and browser extension. It provides fact and image verification services - https://www.logically.ai/. It employs AI as part of its automated search assistant feature. Logically also relies on human fact checkers to assist those who use the service.

Its AI is designed to analyze claims, opinions, and events. It monitors more than one million web domains and social media platforms in real-time, using the information it gathers to assess the veracity of information and assertions on the web.

6. Fullfact

https://fullfact.org/about/ai/ is a media company founded in 2009. It offers several fact-checking tools, including ones that are automated through the use of artificial intelligence. It is a winner of the 2019 Google AI Impact Challenge.

7. Grover

https://grover.allenai.org/ is a fake news detection AI model produced by researchers at the University of Washington. The project was unveiled in 2019, the algorithm takes on the language of specific publications in order to detect misinformation more accurately.

8. Sensity AI

https://sensity.ai/ is a tool for detecting a relatively new frontier in fake information: deepfakes. Unlike written information, it may be more difficult for the untrained eye to determine whether deepfakes are, in fact, deepfakes rather than legitimate images or videos. (Fig.1)

Founded in 2018, Sensity AI may become increasingly useful as deepfakes become more sophisticated, and could be used for reputation attacks, false reporting, and other nefarious ends. Sensity AI assesses and detects the severity of "visual threats". Its detection API combines video forensics and computer vision to determine whether still images or videos or legitimate or fake.

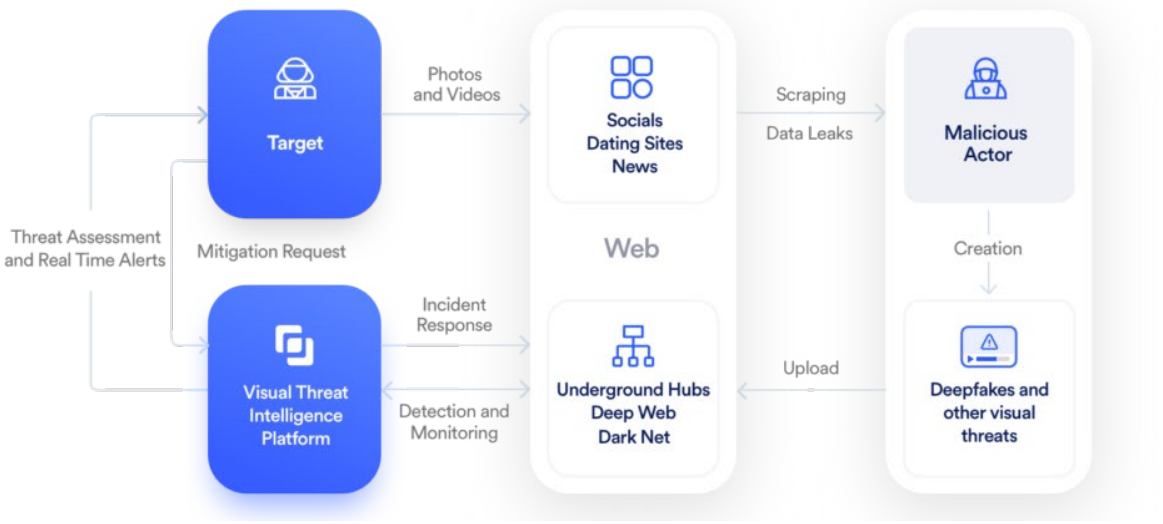


Fig.1. Sensity AI

9. ClaimBuster

https://idir.uta.edu/claimbuster/ is an online tool for instant fact-checking that was founded in 2017. Using Google Fact-Check Explorer API, ClaimBuster allows users to check the veracity of their own text. It gathers search results like their written claim along with determinations of those statements' relative truth of the falsity. (Fig. 2)

ClaimBuster also monitors political debates, relying on AI to highlight claims that it believes are fact-check worthy.

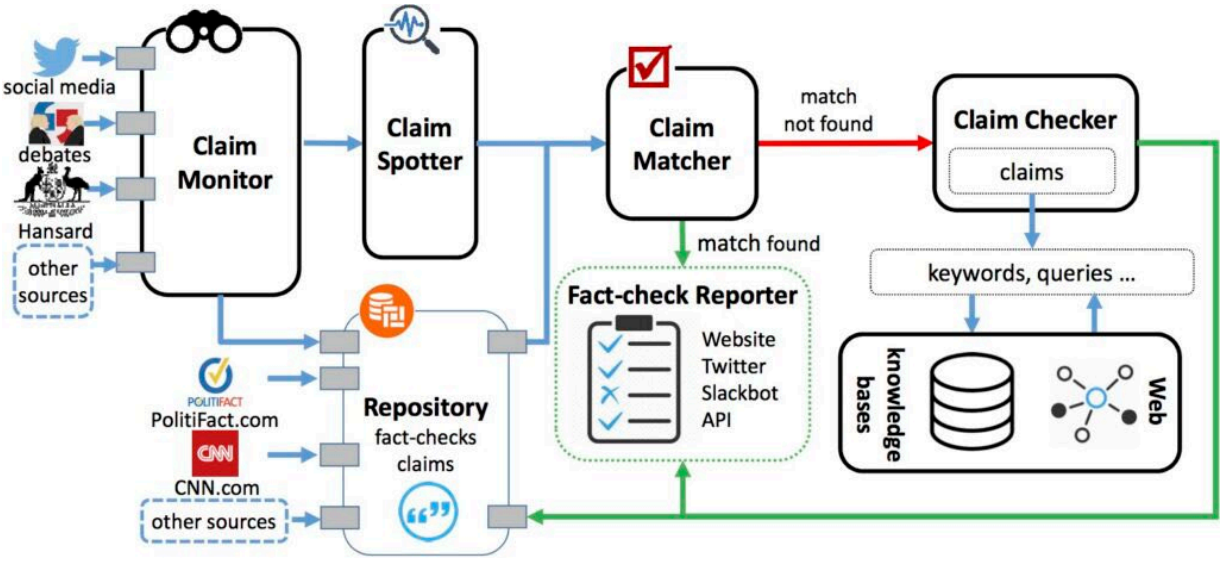


Fig. 2. ClaimBuster

Conclusion

Based on the analysis of existing methods and technologies, it is concluded that traditional methods have limitations in verifying the credibility of information on the internet.

The capabilities of AI in verifying the credibility of information on the internet is demonstrated through the explanation of AI technologies.

From the presented examples of successful applications of artificial intelligence in the verification of the credibility of information on the Internet, it can be concluded that artificial intelligence has a significant potential to help combat disinformation in the online environment.

The effectiveness of AI in verifying the credibility of information on the internet is evaluated as highly promising. However, further efforts and innovation are still needed to ensure that these applications are effective and reliable in the long term.

References

[1] DIMOV, P. (2022) Psychology of Fake News *https://postvai.com/fake/fake-psihologia.html*, 28.01.2024.

[2] GUPTA, S. (2018) Sentiment Analysis: Concept, Analysis and Applications, https://towardsdatascience.com/sentiment-analysis-concept-analysis-and-applications-6c94d6f58c17, 28.01.2024.

[3] IBM TEAM (2022) What is a knowledge graph, *https://www.ibm.com/topics/knowledge-graph#:~:text=A%20knowledge%20graph%2C%20also%20known,the%20term%20knowledge%20%E2%80%9Cgraph.%E2%80%9D*, , 28.01.2024.

[4] IBM TEAM (2022) What is machine learning, *https://www.ibm.com/topics/machine-learning*, 28.01.2024.
[5] LUTKEVICH, B. (2023) Natural language processing (NLP) *https://www.techtarget.com/searchenterpriseai/definition/natural-language-processing-NLP*, 28.01.2024.
[6] VAN DER LANS, S. (2021) 13 AI-Powered Tools for Fighting Fake News *https://thetrustedweb.org/ai-powered-tools-for-fighting-fake-news/,* 28.01.2024.

BLOCKCHAIN TOKENIZATION, ANALYSIS OF TOKEN STANDARDS, ISSUES, AND PERSPECTIVES

Mykola MALENKO (postgraduate)[1]
Yevheniia SHABALA (PhD, associate professor)[2]

[1] *Kyiv National University of Contracture and Architecture, Faculty of Automation and Information Technologies, Department of Cyber Security and Computer Engineering, Kyiv, Ukraine*
[2] *Kyiv National University of Contracture and Architecture, Faculty of Automation and Information Technologies, Department of Cyber Security and Computer Engineering, Kyiv, Ukraine*
[1] malenko.mv@knuba.edu.ua, [2] shabala.ieie@knuba.edu.ua

Abstract
This paper aims to investigate and analyze various aspects of blockchain tokenization, including token standards, their challenges, and prospects. It examines primary standards such as ERC-20, ERC-721, and their derivatives, their impact on the market, and potential implementations. The paper also conducts an analysis of issues related to tokenization and possible solutions. The future prospects of tokenization, their ability to transform various industries, and create new opportunities for innovation and development are also considered.

Introduction

In a world where digital technologies are rapidly changing the landscape of business and finance, blockchain tokenization stands out as one of the most progressive and discussed phenomena. With the growing popularity of cryptocurrencies and the emergence of various blockchain platforms, tokenization is becoming a key element in realizing the potential of decentralized technologies.

Tokenization is the process of converting rights to assets or access to services into digital tokens that exist on a blockchain. This process paves the way for the creation of a digital counterpart to real assets, such as real estate, securities, artworks, or even intellectual property. Thanks to tokenization, such assets become more liquid, accessible, and easier to circulate.

The development of tokenization is closely related to the history of blockchain technology. From the birth of the first blockchain as the technological foundation for Bitcoin to today's multi-functional platforms such as Ethereum [1], blockchain has demonstrated its ability to revolutionize the ways in which we interact with digital assets.

Today, tokenization plays an important role in the development of concepts such as decentralized finance (DeFi) and non-fungible tokens (NFTs). DeFi [2] uses blockchain to create financial systems that operate without traditional intermediaries such as banks or exchanges, while NFTs open up new opportunities for digital art and intellectual property, ensuring uniqueness and ownership of digital content.

Token origin

A blockchain token is a type of digital asset that exists on the blockchain. These tokens can be used for a variety of purposes, including representing assets, means of exchange, rights to assets, or access to certain features or services. They are an important component of the blockchain ecosystem, can serve to create decentralized applications and systems, and are the basis of tokennomics of any crypto project.

The process of creating a blockchain token is called "tokenization" and consists of four main stages: choosing a blockchain platform; development of a smart contract; issuance of tokens; integration with applications and services.

Let's consider each stage in more detail. The first step is to choose a blockchain platform. Different blockchains have different capabilities and characteristics. Today, the most popular blockchain for deploying new tokens is Ethereum, thanks to its flexible smart contract system and large community. Tron, Solana, Binance Smart Chain, and Layer 2 blockchains are also popular choices for creating tokens. The next stage is the development of the necessary smart contracts - programs integrated into the blockchain, which are responsible for the mechanisms of creating tokens, the principles of their distribution among network participants, regulation of the number and other operations specific to a particular token. After the smart contract is developed and placed on the blockchain, tokens are issued. This process may include the distribution of tokens to investors, project founders, or their sale through an Initial Coin Offering (ICO). After creation, tokens can be integrated with various applications and services on the blockchain. For example, they can be used within decentralized financial services (DeFi) and decentralized applications (Daps) for exchange operations, lending or as part of voting mechanisms in project management.

Blockchain tokens are divided into 4 types: cryptocurrency; utilitarian; security; non-fungible (NFT). The first are tokens that function as independent currencies, for example, Bitcoin, Litecoin, Ether. Utility tokens provide access to certain services and functions within the platform. As an example, ApeCoin [3], which was created for the Bored Ape Yacht Club, is used for infrastructure purposes and for project management voting. Another example is the Basic Attention Token (BAT), which is used to thank and encourage users of applications and services that are integrated with BAT. Security tokens, in turn, are used as investment instruments. Such tokens are usually regulated by financial regulators because they contain the characteristics of traditional securities. An example of this type is the BCAP [4] token, it is based on the Ethereum blockchain and is the first case of venture fund tokenization. The last type are non-fungible tokens, they are unique and cannot be exchanged for other tokens on equal terms. They are often used to represent digital art, collectibles, intellectual property rights, and other unique assets. An example of such a token is the first Quartz News article [5], which was wrapped in an NFT and sold for 1 ETH.

According to the token monitoring service Token Sniffer [6], there are currently about three and a half million different tokens, which indicates the active development of the crypto industry.

Token standardization

With the increase in the number and functional diversity of blockchain tokens, there is a need for their standardization. Standards define rules and protocols, ensure unification, compatibility of tokens and their interoperability between various blockchain applications and services. The main aspects of the token standard include:

- functionality;
- compatibility;
- security and transparency;
- interoperability;
- specific characteristics;
- regulatory requirements;
- extensions and modifications.

The functional aspect of the standard defines how tokens can be transferred, how balance information can be obtained, and what actions can be performed with the tokens. For example, the ERC-20 standard defines functions for transferring tokens, obtaining a token balance, and determining the total number of tokens. The compatibility of the standard ensures that the token can interact with various smart contracts and blockchain applications that support this standard. A token created according to a certain standard will be supported by all wallets, exchanges and other decentralized services that support this standard. Security and transparency standards determine how information about tokens should be stored, and how interaction between different network participants should take place, thus ensuring protection against fraud and abuse. A token standard may include specifications to enable token interoperability between different blockchains or layers in a network, allowing for flexibility and wider usage. Depending on the standard, tokens may have specific characteristics, such as uniqueness (for NFTs), the ability to delegate rights (e.g. in DeFi standards), or special rules for issuance and management (as in the case of security tokens. Certain token standards take into account regulatory requirements , especially in the case of security tokens and those representing securities or other regulated financial instruments. This may include rules for tracking token holders, requirements for their sale, or transfer restrictions. Token standards may also allow for expansion or modification, allowing developers to add new functions or adapt existing standards to specific project needs.

The most known standards are ERC-20 and ERC-721 [7] on Ethereum blockchain. The first is a standard for creating fungible tokens that can be used as currency, represent company shares, or be part of a loyalty system. ERC-20 defines a set of rules that each token must comply with, ensuring their compatibility with other products and

services that run on Ethereum. This includes methods for transferring tokens, obtaining data about total and available tokens, and information about owners and their balances.

The ERC-721 standard is the basis for non-fungible tokens (NFTs). Its difference is that each token is unique and cannot be replaced by another token. This is ideal for representing ownership of unique objects such as works of art, collectibles, or even digital property in virtual worlds.

There are also many standards that are built on the basis of ERC-20, ERC-721 and created to expand their capabilities, in particular: ERC-223, ERC-777, ERC-809, ERC-998, ERC-1400 and others.

Each of these standards plays an important role in the development of the blockchain ecosystem, allowing the creation of various types of tokenized assets and their interaction within various blockchain applications and platforms. They contribute to innovation and expansion of blockchain technologies in finance, digital arts, intellectual property and many other areas.

Tokenization issues and perspectives

Blockchain tokenization offers new horizons in efficiency and asset availability, but also comes with a unique set of challenges.

One of the main challenges of tokenization is the regulatory landscape. Due to the novelty and speed of development of digital assets, many countries have not yet had time to develop clear legislation regulating this area. This creates legal uncertainty that can inhibit the development and adoption of tokenized assets, and increases risks for investors.

Technical aspects also represent a significant barrier. Integrating blockchain with existing financial systems requires significant technical resources and expertise. In addition, security issues are important, as digital tokens, like any other digital asset, are exposed to the risks of cyber attacks and fraud, according to the Token Sniffer service, approximately one seventh of all tokens created have a purely fraudulent function.

However, despite these challenges, the prospects for tokenization are quite promising. One of the main advantages is the reduction of barriers to market entry, which allows a wider range of investors to invest in a variety of assets. Tokenization also provides a higher degree of transparency and efficiency in asset management, thanks to the immutability and transparency of the blockchain.

Another important aspect is the possibility of fractional ownership, which allows investors to buy shares in assets that were previously inaccessible due to high costs. This could radically change the investment landscape, making high-value assets such as real estate or art accessible to a wider range of investors.

Conclusion

Blockchain tokenization is the transformation of traditional assets or property rights into digital tokens that exist on the blockchain. This process opens up new opportunities for investment, democratizing access to assets and ensuring transparency and efficiency of transactions.

Analysis of tokenization standards indicates the need for harmonization and standardization in this area. Standards such as ERC-20 or ERC-721 on the Ethereum network already provide a certain level of unification, but need further adaptation and development to cope with the diversity of assets and their specific requirements.

The issue of blockchain tokenization consists in solving regulatory issues, ensuring a high level of cyber security, and integration with existing financial systems.

Despite these challenges, the prospects for blockchain tokenization remain significant. This process offers new opportunities for the global economy, including improving asset liquidity, reducing transaction costs, and creating new markets for previously illiquid assets. Innovations in tokenization have the potential to radically change the way we interact with assets, paving the way for more inclusive and efficient financial systems.

References

[1] Intro To Ethereum, https://ethereum.org/developers/docs/intro-to-ethereum.
[2] Decentralized Finance (DeFi) Policy-Maker Toolkit, WEF 2021, https://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf.
[3] ApeCoin ABOUT section, https://apecoin.com/about.
[4] Blockchain Capital, About section, BCAP build section, https://www.blockchaincapital.com/about-us.
[5] We sold the first-ever NFT news article for $1,800, https://qz.com/1984094/quartz-is-selling-the-first-ever-nft-news-article.
[6] Token Sniffer, actively monitoring, https://tokensniffer.com/.
[7] Token Standards, https://ethereum.org/developers/docs/standards/tokens.

IMPROVING THE EFFICIENCY OF ORGANIZATIONAL SUPPORT AND MANAGEMENT OF REGIONAL AIR TRAFFIC

Oleksandra LIUBYCH (cadet)

Flight Academy of the National Aviation University, educational degree "Master" in specialty 272 "Aviation transport"
oleksandralul@gmail.com

Abstract

Air transport is a very important component. It makes life much easier and faster. Because it has major advantages over other modes of transportation around the world:

- Passengers and their cargo move much faster.
- The travel distance is reduced.

Aviation, as a branch of engineering devoted to the design, modeling, and use of aircraft, is an important part of air transportation. We owe it to aviation that we are able to travel between countries in a matter of hours, but unfortunately, regional air service is very poorly developed in Ukraine.

Keywords

Passengers, air transportation, aircraft, air transportation, airline, aircraft type.

Introduction.

Our modern world is developing every day and is becoming more progressive and modernized than yesterday. For a comfortable existence, humanity needs a lot of factors. One of them is transportation. There are five main types of transportation in the world. Their distribution is determined by the difference in the vehicles used to move cargo and passengers, as well as the different natural environments in which they are used for operation. Ukraine's transportation system is a large and complex economic complex located throughout the country. It consists of: land transport, namely: rail and road, water transport, including sea and river, air transport and pipeline transport.

The concept of "air transport" exists directly as an alternative to land and water transport, in the case when it is necessary to quickly change the location of a person or cargo, but the price of such an opportunity is appropriate, that is, more expensive than in the use of other modes of transport.

Aviation, as a branch of engineering devoted to the development, modeling and use of aircraft, is an important part of air transportation. Aviation activities are divided into civil aviation, which includes general and commercial aviation, and military aviation.

One of the key objectives of civil aviation is to meet the needs for air transportation by providing safe and economical transportation of passengers, baggage and cargo. Types of air transportation include domestic and international, as well as scheduled and non-scheduled flights.

Scheduled air transportation is carried out in accordance with the published schedule, including additional flights. Irregular transportation takes place on charter flights under agreements between the customer and the airline.

The special role of air transport is also determined by the frequency and versatility of transportation, which in most cases is independent of the time of year and climatic conditions, and when weather conditions interfere with the operation of airports, no other mode of transport can function due to the same weather-related obstacles.

The term "air transport" is widely used in practice and describes the transportation industry as an activity carried out in airspace using aircraft.

The term "aviation" is traditionally used to refer to activities in airspace.

Aviation is a branch of engineering that is directly related to the development, modeling, design, and then use of aircraft that are heavier than air. The word "heavier than air" is especially important, because otherwise, knowing physics, it would be impossible to get up in the air. However, thanks to a large number of scientists and inventors, most of whom unfortunately never got to experience the same feeling of flight and died developing and testing their inventions, but thanks to them we have this opportunity.

Aviation activities have different goals, objectives and means of implementation. One of the most important goals of aviation activity is to meet the interests and needs of individuals and legal entities in air transportation, to protect their rights to safe, high-quality and economical air transportation. This goal is realized through the use of civil aviation, which in turn is subdivided into general aviation, which is used on a free-of-charge basis, and commercial civil aviation. The main purpose of commercial civil aviation is to provide air transportation of passengers, baggage and cargo for a fee.

Air transportation is defined as "transportation of cargo or a person in the airspace, carried out by means of aircraft movement in the airspace".

International air transportation is a type of transportation in which the points of departure and destination, regardless of whether there is or is not a break in transportation or transshipment, are located, respectively, either on the territories of several states or on the territory of one state, if a landing point is provided in a foreign state.

Domestic air transportation, in turn, can be regular and irregular.

Scheduled air transportation - transportation carried out on scheduled flights, i.e. on flights of aircraft operated in accordance with the schedule published in the prescribed manner, including transportation on additional flights, i.e. on flights operated in addition to the schedule on the dates and on the same route as the scheduled flight.

Irregular air transportation - transportation performed on irregular (charter) flights, i.e. on flights of aircraft operated outside the published schedule in accordance with the air transportation agreement concluded between the customer and the airline or other operator.

Domestic air transportation can also be considered and called regional or intra-regional.

Regional air transportation is domestic air transportation that is carried out according to regular and permanent schedules established and available to everyone on the websites of airlines and airports.

Airlines in Ukraine have a lot of contracts with other countries and have established international transportation, but not regional air connections.

Ukraine has a huge base of airports that would be great to restore and start operating regional air services.

This will primarily bring not only income to the airlines themselves, but also boost the economy in the country.

So I suggest starting with the airport in Kropyvnytskyi. Kropyvnytskyi, and until 2014 Kirovohrad, is a modern and developing city. It is small, cozy, and most importantly, compact, which will not cause a problem to quickly get to the airport for your flight. Most importantly, the city is home to a university that has been one of the best in Ukraine for training qualified civil aviation professionals for over 70 years. This is the Flight Academy of the National Aviation University. It is a higher education institution that trains cadets who will become the best pilots, dispatchers, aviation technicians and aviation production managers in the future. And the most important thing in this institution is its pride, namely its teachers, who are simply the best professionals in their field. And to operate flights from Kropyvnytskyi to Kyiv.

In order to determine the cost of such a flight, it is necessary to calculate the ACMI, which is the cost of a flight hour under ACMI (Aircraft Crew Maintenance Insurance), which is calculated from the following four steps:

1) A - aircraft is the calculation of depreciation charges for the aircraft for the renovation of the airframe and engines.

This indicator can be determined by the actual hours flown per year (Tg) and the depreciation rate calculated from the aircraft's service life. This indicator is assumed to be 25 years of operation or 4% of the depreciation charges of the initial cost of the aircraft. The annual flight time is: Tg = 1000 hours,

$$A = 0.04 \cdot Vps / Tg = 0.04 \cdot 55000000 / 1000 = 2200 \text{ USD/hour}$$

2) C - crew is an indicator of the need for personnel and the level of wage costs for flight and engineering staff:

Travel expenses per hour of annual flight time:

$$C = n \cdot 365 \cdot Wh / Tg,$$

where n is the number of crew members;

365 is the number of days in a year;

Bwd is the business trip payment rate per person = $80.

That is, the business trip payment per hour of annual flight time will be equal to:

$$C = 2 \cdot 365 \cdot 80 / 1000 = 58.4 \text{ dollars per hour}$$

The payroll for the flight crew and engineering and technical personnel involved in the maintenance of this aircraft will be calculated on average for the year based on the average salary of a crew member of $3000 without a breakdown by position on average for the year and will be converted to one hour of annual flight time:

$$FTE = 2 \cdot 12 \cdot 3000 / 1000 = \$72/hour$$

So: C = 58.4 + 72 = 130.4 (dollars/hour)

Next:

3) M-maintenance, is an indicator of the necessary costs associated with the maintenance of a given aircraft per hour of flight time. To determine this indicator, it is necessary to calculate the labor intensity of the maintenance process based on the existing conditions of the design life of the airframe and engines.

M-maintenance is 1/3 of A-aircraft and is measured in dollars/hour:

$$M = 2200 / 3 = 733 \text{ USD/hour.}$$

4) I-insurance is an indicator of the sum of all types of insurance per flight hour: namely, third-party insurance, crew insurance, hull insurance, etc.

The amount of insurance payments is 3% of the initial cost of the aircraft:

$$I = 0.03 \cdot Vps / Tr = 0.03 \cdot 55000000 / 1000 = 1650 \text{ USD/hour.}$$

You can calculate flight fuel consumption using the following formula:
Let's take the cost of fuel, for example, as USD 270 (excluding VAT), which is a typical price at Boryspil Airport. In this case, the fuel costs will be:

$$5.62 \times 270 = 1420.2 \text{ (dollars)}$$

If the profitability is 20% (or USD 425.9), then the airline's profit from one flight will be equal to USD 7151.0.
Such a regional flight on the Kyiv-Kropyvnytskyi-Kyiv route can be operated 3 times a week by order of Sky UP. And in the future, much more. Due to the large number of people who want to save their time and money.

Conclusions

In this paper calculates whether regional air services are profitable for Ukrainian air carriers and whether they should be renewed. The analysis of Ukraine's aviation system showed that it is necessary, because international air travel is well taxed, and there are many abandoned airports in the rest of the country. Regional transportation should become more important for airlines, as it provides a guaranteed increase in the efficiency of the airline's operations and access to a higher level of competitiveness and, above

all, the development of the country. It can also be concluded that the resource costs are quite affordable for the airline to use.

Based on the calculation of the flight from Kropyvnytskyi to Kyiv, we can conclude that it is very cost-effective. Passengers spend more than 5 hours traveling between these cities, which is much less profitable than spending 1-2 hours paying the same money.

References

[1] Spivak S.N. Logistic approach in the system of management of air transportation flows of air transportation. Scientific Bulletin of MSTU GA. URL: https://cyberleninka.ru/article/n/logisticheskiy-podhod-v-sisteme-upravleniya-potokami-vozdushnogo-transporta/viewer.

[2] State Enterprise for Air Traffic Services of Ukraine. URL: http://uksatse.ua/index.php.

[3] Galyamova T.V. ORGANIZATION OF TRANSPORTATION BY AIR. URL:http://spbguga./files/2018/ZF/Metod_materi/Organiz_perevozok_na_vt_lektsii.pdf.

ISSUES OF ENSURING CYBERSECURITY IN INDUSTRIAL INTERNET OF THINGS OBJECTS

Maksym DELEMBOVSKYI (candidate of technical sciences, associate professor)[1]
Borys KORNIICHUK (candidate of technical sciences, associate professor)[2]
Mykola KLYMENKO (candidate of technical sciences, associate professor)[3]

[1] *Kyiv National University of Construction and Architecture, Faculty of Automation and Information Technologies, associate professor of the department of cybersecurity and computer engineering, Kyiv, Ukraine*
[2] *Kyiv National University of Construction and Architecture, Faculty of Automation and Information Technologies, associate professor of the department of vocational education, Kyiv, Ukraine*
[3] *Kyiv National University of Construction and Architecture, Faculty of Automation and Information Technologies, associate professor of the department of machinery and equipment for technological processes, Kyiv, Ukraine*
[1] delembovskyi.mm@knuba.edu.ua, [2] korniichuk.bv@knuba.edu.ua, [3] klymenko.mo@knuba.edu.ua

Abstract

This work focuses on the importance of cybersecurity within the context of the Industrial Internet of Things (IIoT). The Industrial Internet of Things refers to the application of the Internet of Things (IoT) in manufacturing processes and industry, where machines and equipment are networked to optimize production, increase efficiency, and reduce costs. However, the growth in connected devices significantly increases potential vulnerabilities to cyber-attacks. The paper examines various threats to IIoT, such as unauthorized access, data breaches, viruses, and malicious software. Protection strategies are discussed, including data encryption, user authentication, and regular security updates. Special attention is given to the analysis of cyber attack cases on industrial sites and learning lessons from these incidents. The work concludes with recommendations for developing more attack-resistant IIoT systems and ways to ensure ongoing cybersecurity in a dynamically changing digital world.

Introduction

It is important to emphasize the rapid development and integration of Internet of Things (IoT) technologies in the industrial sector. The Industrial Internet of Things (IIoT) is becoming a key element in modern manufacturing industry, as it provides process automation, increases work efficiency, and contributes to the innovative development of enterprises. However, alongside the advantages offered by IIoT, the risk of cyber threats is also increasing. These threats can have serious consequences, including the loss of confidential information, interruptions in manufacturing processes, and even physical damage to equipment. This work aims to explore the key aspects of ensuring cybersecurity in IIoT objects. We will consider potential cyber threats and vulnerabilities that industrial systems face, as well as strategies and practices that can be used to strengthen cybersecurity in this area. An important aspect of the study is the analysis of current challenges and the development of recommendations for enterprises on

effective cybersecurity management in the context of rapid technological development. Main part. Some of the latest events in the global cyberspace, which clearly indicate the activity of attacks on the Industrial Internet of Things, can be easily analyzed from open data. Thus, the information about the attack on such objects [1-3], namely:

1. Colonial Pipeline. The Colonial Pipeline company suffered an attack by Russian cybercriminals from the "DarkSide" group, which led to the cessation of fuel supplies across the entire Eastern US coast. The company had to pay a ransom of 5 million US dollars.
2. JBS USA. The world's largest meat processing company, JBS USA, paid almost 11 million US dollars in Bitcoin after a cyberattack that led to the shutdown of operations in Australia, Canada, and the US.
3. Kaseya. The company Kaseya experienced a cyberattack at the beginning of July, which affected numerous managed service providers and their clients. It is estimated that about 1500 small and medium-sized companies suffered damages due to this attack.
4. Brenntag. The German chemical distribution company, Brenntag, suffered an attack using "DarkSide" ransomware, which targeted its North American division, resulting in the loss of 150 GB of data.

This is far from an exhaustive list of companies that could be subjected to such types of attacks. Therefore, this work specifically considers one of the approaches to organizing the security of the Industrial Internet of Things. Growth of IoT and increase in the number of attacks. According to ThreatLabz research, there is an 18% increase in IoT device traffic compared to previous estimates in 2021. At the same time, the number of attacks on IoT devices has increased by 400%. Among the dominant threats are botnets, such as Mirai and Gafgyt, which account for 66% of all attacks. According to the study, the manufacturing sector is the main target. The manufacturing sector leads in the amount of unique IoT traffic, almost tripling the number of other sectors. The manufacturing sector faces more than three times the number of attacks compared to other industries, accounting for 54.5% of all attacks on production. The US as the main target for malware developers. The US attracts most malware authors due to its developed digital infrastructure. According to certain companies, the main methods are IoT infections. According to the study, the two main methods of infecting IoT devices are brute-forcing weak passwords and exploiting vulnerabilities in network services. In the first half of 2023, 97.91% of brute-force password attempts were targeted at the Telnet protocol. To ensure cybersecurity in Industrial Internet of Things objects, it is important to perform a number of basic tasks [1-3]:

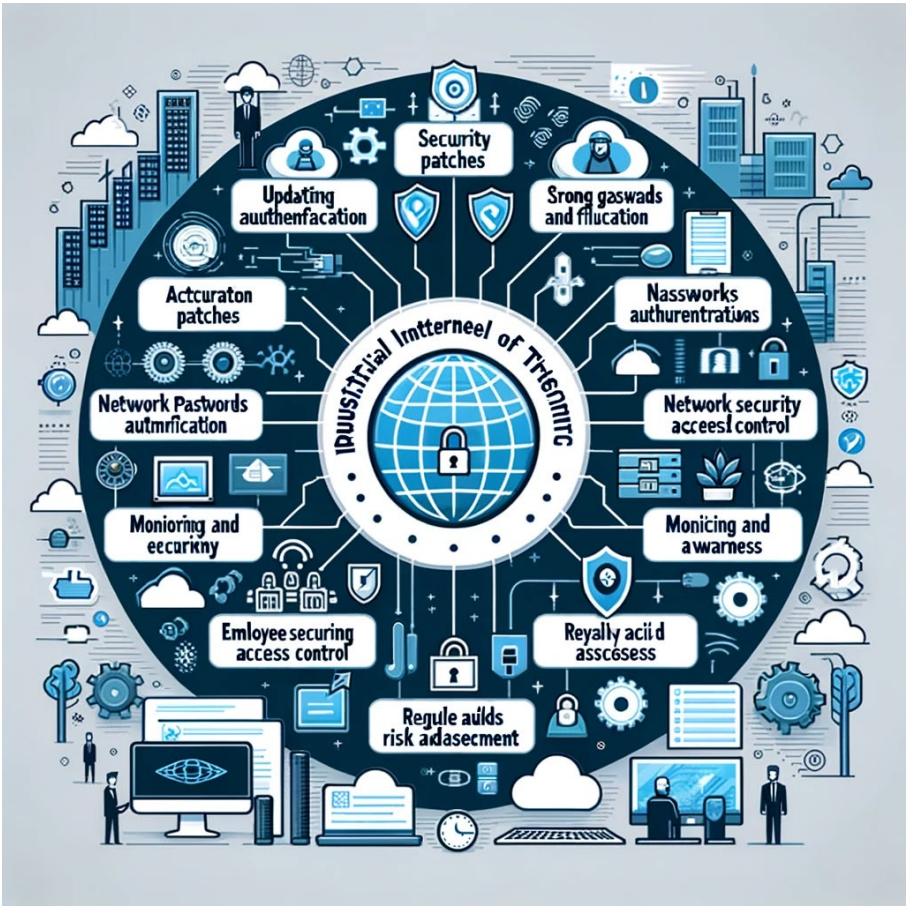


Fig. 1. Fundamental tasks for ensuring cybersecurity in IIoT

1. Updates and security patches. Regularly update all devices and systems, including firmware, to protect against known vulnerabilities.
2. Strong passwords and authentication policies. Use complex passwords and change them regularly. Apply multi-factor authentication for an additional layer of protection.
3. Network security and traffic filtering. Install firewalls and intrusion detection and prevention systems (IDS/IPS) to monitor and control network traffic.
4. Data encryption. Ensure data encryption during transmission and storage to protect against unauthorized access or information leakage.
5. Monitoring and access management. Use monitoring systems to detect suspicious behavior and manage access to systems and data.
6. Physical security. Ensure physical protection of critical infrastructure components to prevent unauthorized physical access.
7. Education and staff awareness. Train staff in cybersecurity basics and best practices to prevent human errors that could lead to security incidents.
8. Regular audits and risk assessment. Conduct regular security audits to identify and mitigate vulnerabilities, and assess risks to identify potential threats.

Conclusion. With the increasing implementation of IIoT technologies in various industrial sectors, the number of potential attack vectors for cybercriminals significantly

increases. The main challenges facing IIoT in cybersecurity include protection against vulnerabilities related to weak passwords, exploitation of network services, botnet attacks, and malware dissemination. Special attention is focused on the manufacturing sector, which is one of the main targets of cyberattacks. It emphasizes the importance of regular software updates, the use of complex passwords, data encryption, and the development of comprehensive cybersecurity strategies that include network monitoring, security audits, and staff training. For more effective cybersecurity in IIoT, it is crucial to integrate multi-layered security measures, including physical protection, network security, access management, and incident response. Additionally, considering the specificities of particular industries will allow for the development of more precise and effective cyber defense strategies. In the context of rapid digital technology development and the increasing number of connected devices, the importance of cybersecurity issues in IIoT will continue to grow, requiring companies to constantly pay attention and adapt to new challenges in this area.

References

[1] Cybersecurity Trends to Prepare for in 2022. Recap of Cybersecurity and Cyber Attacks in 2021: https://iiot-world.com/ics-security/cybersecurity/cybersecurity-trends-to-prepare-for-in-2022 01.03.2022.

[2] Делембовський, М., & Корнійчук, Б. (2023). Аналіз сучасних наукових публікацій за напрямком тематики кібербезпеки iot технологій. Grail of Science, (25), 203-206.

[3] Belov, A., Delembovsky, M., & Shklyar, V. (2021). Моделювання кіберзагроз для Інтернет речей. Transfer of innovative technologies, 92-94.

APPLICATION OF ARTIFICIAL INTELLIGENCE IN INTERNET OF THINGS SYSTEMS

Mechyslav LOSOVSKYI (Bachelor's degree student)

Kyiv National University of Construction and Architecture, Faculty of Automation and Information Technologies, Department of Cybersecurity and Computer Engineering, Kyiv, Ukraine
losovskyi_mb@knuba.edu.ua

Abstract
This work provides an overview of the integration of Artificial Intelligence (AI) into the Internet of Things (IoT), with a focus on global trends, applications, challenges, and the future outlook of these technologies.

Introduction

Artificial Intelligence (AI) and the Internet of Things (IoT) are two cutting-edge technologies that are rapidly transforming the world around us. AI enables machines to learn from experience, adapt to new inputs, and perform human-like tasks, while IoT connects physical objects to the internet, allowing them to collect and exchange data. The integration of AI into IoT opens up limitless possibilities for automation, data analysis, and intelligent system management.

Artificial Intelligence is a branch of computer science concerned with creating machines capable of mimicking human thinking and behavior. Key components of AI include machine learning (ML), neural networks, deep learning, natural language processing, and cognitive computing.

The Internet of Things connects physical objects ("things") capable of collecting and exchanging data over the internet. IoT devices can range from simple temperature sensors to complex machines that collect vast amounts of data for analysis and decision-making.

The integration of AI into IoT significantly enhances data analysis capabilities. Machine learning allows systems to identify patterns and anomalies in data from IoT devices, which can be used for predicting future trends, optimizing processes, and automating decisions without direct human intervention.

AI can significantly improve the efficiency of automation and control in IoT systems. This is achieved through automated decision-making based on real-time data analysis. For example, intelligent energy management in buildings can reduce electricity costs, and automating production lines using AI can increase productivity and reduce health risks for workers.

The integration of AI into IoT has significant potential to improve system security. AI can analyze data from IoT devices in real-time to identify potential threats and vulnerabilities, such as unauthorized access or anomalous behavioral patterns, allowing

systems to automatically prevent or respond to these threats. The use of machine learning algorithms to recognize security patterns can greatly reduce the risk of cyberattacks and protect confidential data.

AI plays a key role in transforming large volumes of data collected from IoT devices into actionable insights. Using techniques for intelligent data analysis and machine learning can help organizations make informed decisions, improve products and services, and identify new business opportunities. For example, analyzing energy consumption data can help develop more efficient energy management strategies.

AI and IoT together are transforming residential environments and urban landscapes, creating smart homes and automated cities. In smart homes, AI is used to manage lighting, temperature, security, and other systems to enhance comfort, efficiency, and energy savings. In automated cities, AI helps manage traffic flows, monitor environmental conditions, and optimize municipal services, improving residents' quality of life and reducing environmental impact.

These aspects demonstrate how AI can provide intelligent management and analysis in IoT systems, offering innovative solutions for security, data analysis, and everyday comfort. The integration of these technologies continues to open new horizons for innovation across various fields.

The Industrial Internet of Things (IIoT) represents a significant application area where AI and IoT converge to revolutionize manufacturing and production processes. By integrating AI into IIoT, industries can achieve unprecedented levels of efficiency, productivity, and safety. AI algorithms can predict equipment failures before they occur, optimize production schedules for maximum efficiency, and ensure quality control through real-time monitoring and analysis. This proactive approach to maintenance and production management not only reduces downtime but also extends the lifespan of machinery and reduces operational costs.

While the integration of AI into IoT offers numerous benefits, it also presents several challenges and limitations. Privacy and data security emerge as primary concerns, as increased connectivity and data collection raise the risk of personal information being compromised. Additionally, the deployment of AI and IoT technologies involves significant infrastructure and investment costs, and there may be technical challenges related to interoperability, scalability, and managing the vast amounts of data generated by IoT devices. Ethical considerations also come into play, particularly in terms of decision-making autonomy and the potential for job displacement in certain sectors due to automation.

Conclusion

Looking ahead, the future of AI and IoT is poised for continued growth and innovation. Emerging technologies such as 5G networks, edge computing, and blockchain are expected to further enhance the capabilities and applications of AI in IoT by facilitating faster data processing, improved security, and better device connectivity. The

development of more advanced AI algorithms and the increasing ubiquity of IoT devices will enable more sophisticated and autonomous systems, ranging from self-driving cars to fully automated smart cities and factories. As these technologies evolve, they will undoubtedly create new opportunities and challenges, shaping the future of industries and everyday life.

References

[1] IEEE Xplore Digital Library - https://ieeexplore.ieee.org/.
[2] Google Scholar - https://scholar.google.com/.
[3] ResearchGate - https://www.researchgate.net/.
[4] SpringerLink - https://link.springer.com/.
[5] ScienceDirect - https://www.sciencedirect.com/.

USING THE SMART HOUSE SYSTEM AS A MECHANISM FOR IMPROVING THE HEAT SUPPLY SYSTEM

Anastasia KONDAKOVA (graduate student)

Kyiv National University of Construction and Architecture, Faculty of Automation and Information Technologies, Department of Cybersecurity and Computer Engineering, Kyiv, Ukraine
kondakova_am@knuba.edu.ua

Abstract

Unfortunately, it is unlikely that anyone from Kyiv has never encountered heat supply problems. Cold heating batteries during frost, flooded streets, asphalt collapses, sometimes together with cars, burns to random passers-by, damaged property, the need for constant investment are just some of the problems that the city faces as a result of accidents on the heating network. As Vitrenko, a member of the Kyiv City Council, reported, "In Kyiv, 70% of networks are in an emergency state. A burst valve or pipe can happen anywhere in the capital. We cannot even predict, because of the 2,000 kilometers of Kyiv networks (hot supply and heat supply pipes), 80% have already served more than their service life."

Since the beginning of 2024 alone, there have been 5 critical accidents with property damage and street flooding in the city of Kyiv, namely:

20.01.24 damage on the street Oleksy Tykhoi;

13.01.24 damage on the street Jules Verne;

09.01.24 damage on the street Obolonsk;

07.01.24 damage on the street Jules Verne;

02.01.24 damage on Ave. Desired.

Replacing networks in parts does not give the desired result. Not only new pipes are needed, but also control of pressure, temperature and flow rate directly inside the pipe.

Keyword

Sensor, smart home system, heat supply system.

Introduction

It is necessary to change outdated networks to those that would provide 24/7 monitoring by sensors, transmitting data to a server.

The scenario of the principle of cable operation:

Sensors embedded in the cable inside the pipes continuously measure the pressure, temperature and flow rate of water or coolant in the pipe.

The smart cable is located next to the sensors in the pipe. It is responsible for transmitting real-time data from the sensors to the central control system and transmitting control signals in the reverse direction.

As a result, the sensor detects an abnormal pressure spike, indicating a potential risk of a pipe burst, and transmits it to a smart cable, which in turn transmits pressure spike data to the central control system.

The data transmission system facilitates communication between the smart cable and the central control system. The goal is to provide data, such as pressure spikes, reliably and quickly.

On the side of the monitoring and control center, there should be a remote control center that analyzes input data, makes decisions, and sends control commands. The system analyzes pressure data, determines the risk of a pipe burst and solves the issue of pressure regulation.

Controllers in the pipeline system, located at various control points of the pipeline system, execute commands received from the smart cable.

The feedback loop ensures the desired effect of system settings. The cable is commanded to open the relief valve to reduce the pressure. After adjusting the pressure, the sensors confirm that the pressure is back to normal and transmit this information to the control system.

External interfaces provide points of interaction for service personnel, emergency systems and data analysis tools. Namely, maintenance personnel are notified of an incident for inspection and preventive maintenance.

This scenario illustrates a situation where an intelligent cable system effectively prevents a pipe burst by quickly detecting, reporting and responding to a pressure anomaly in the pipe system.

Conclusions

To improve the situation with heat supply, Ukraine can follow three paths.

1) Open own production of pipes.

The current state of the industry indicates that, although Ukraine has a strong base in traditional pipe manufacturing, the transition to smart pipe manufacturing is likely to require significant investment in new technology, research and development, and possibly collaboration with technology companies specializing in smart infrastructure.

From an economic point of view, the feasibility of manufacturing smart pipes in Ukraine will depend on several factors, including the cost of technological modernization, the availability of skilled workers and the potential market demand for such advanced infrastructure solutions. The initial investment may be high, but the long-term benefits, such as increased efficiency, reduced maintenance costs, and alignment with global smart city trends, can make it worthwhile.

2) Using Smartpipe® technology from Smart Pipe Technologies. This system can be especially useful for Kyiv when restoring old or corroded pipelines, especially in urban or hard-to-reach areas. Given the complex urban environment of Kyiv and the challenges of maintaining and upgrading underground infrastructure, Smartpipe® trenchless technology and the ability to pull through existing pipelines can minimize disruption and installation costs. In addition, its integrated fiber optic monitoring system will increase the probability of error-free leak detection and pipeline safety, which is crucial in densely populated areas.

3) Use of SmartProbe technology from Pipelife. This system can be very useful for improving the management of Kyiv's water supply and heat supply network. The ability of this technology to provide real-time data on various parameters such as pressure, temperature and water quality will help to effectively manage the water distribution system, detect leaks early and ensure water quality. Given the importance of reliable and safe water supply in cities, SmartProbe can play a significant role in improving the management of urban water infrastructure.

Smart home technology can help Ukraine improve the infrastructure of cities and villages, using the example of the city of Kyiv. Taking into account the frequency of necessary debugging work, the implementation of such technology should become quite economically profitable. Currently, we have only 2 smart pipeline technologies in the world.

Countries known for their advancements in smart city technologies, such as Singapore, South Korea, and some cities in Scandinavia, might be exploring or implementing such smart pipe systems. Smart pipe technology for heating systems represents a promising area for urban infrastructure development, its widespread implementation is still in the nascent stages

While the technology for smart heating pipes is available and has been tested in various capacities, its large-scale application in city-wide heating systems like Kyiv's is still in the early stages of development.

References

[1] https://www.smart-pipe.com/
[2] https://www.pipelife.com/
[3] https://t.me/s/kievreal1
[4] https://t.me/s/kiev_infoo

INTEGRATION OF THE INTERNET OF THINGS INTO THE MILITARY AFFAIRS SYSTEM IN UKRAINE

Yevheniia SHABALA (PhD, associate professor)[1]
Anastasia LYSENKO (Student)[2]

Kyiv National University of Construction and Architecture, Faculty of Automation and Information Technologies, Department of Cybersecurity and Computer Engineering, Kyiv, Ukraine

[1] anastasiakazanceva948@gmail.com, [2] shabala.ieie@knuba.edu.ua

Abstract
This study delves into the integration of the Internet of Things (IoT) into Ukraine's military affairs system. It explores the strategic implementation of IoT in Armed Forces operations, emphasizing cybersecurity challenges. The article analyzes the optimization of logistics through IoT solutions and investigates trends in military applications. The research also examines the heightened efficiency of reconnaissance strategies, particularly focusing on the synergies between unmanned aerial vehicles and IoT. Ethical considerations related to IoT integration into military operations are discussed, alongside an exploration of market dynamics. The findings are exemplified through the modernization efforts within the Ukrainian Armed Forces.

Keywords
Integration of IoT, Strategic Implementation, Cybersecurity Challenges, Logistics Optimization, Trends in Military Applications, Efficiency in Reconnaissance, Synergies with UAVs, Ethical Considerations, Market Dynamics, Modernization in Ukrainian Armed Forces.

Introduction

In the contemporary landscape of military affairs, the strategic use of Unmanned Aerial Vehicles (UAVs) has become paramount for various applications. This introduction encompasses a comprehensive exploration of the classification, applications, and challenges associated with UAVs, shedding light on their significance in both forensic and military domains.

Bilous (2016) provides insights into the classification of UAVs and its pivotal role in forensic practice, laying the foundation for understanding their applications in diverse scenarios [1]. Glotov, Gunina, and Telechuk (2017) contribute by analyzing the potential applications of UAVs for military purposes, emphasizing the importance of UAV technology in modern warfare [2].

Grebenikov et al. (2009) delve into the challenges faced by Unmanned Aeronautical Complexes in Ukraine, offering a comprehensive perspective on the issues surrounding UAV development and integration [3]. Minochkin et al. (2017) explore the use of

UAVs as retransmitters of tactical mobile radio networks, showcasing their versatility in military communication systems [4].

Nalivayko et al. (2009) highlight the features of NATO Air Force tactics within suppressed integrated air defense systems, underscoring the strategic implications of UAV deployment [5]. Stetsenko, Danik, and Pastushenko (2004) provide a handbook on space systems supporting unmanned vehicles, contributing to the foundational knowledge of UAV technologies [6]. Kozhedub Kharkiv University of Air Force [7]. Tsimbalistova (2015) explores the development of the UAV services market, reflecting the innovative progress in modern aviation [8].

Shulezhko (2013) outlines basic directions for the development and application of UAVs, providing a comprehensive guide [9]. Clothier (2011) contributes to the effective classification of UAVs, emphasizing airworthiness and operational regulations [10].

Hlotov et al. (2018) focus on the development and investigation of UAVs for aerial surveying, presenting advancements in this critical application area [11]. Meyer-Fujara (n.d.) explores the broad applications of military and non-military UAVs, contributing valuable perspectives [12].

Watts, Ambrosia, and Hinkley (2012) delve into the role of UAVs in remote sensing and scientific research, providing a comprehensive classification and considerations for their use [13].

Collectively, these references form the foundation for a thorough exploration of UAVs in both forensic and military contexts, setting the stage for a detailed analysis of their classifications, applications, and emerging trends.

Methods of Applying Unmanned Aerial Vehicles (UAVs) in the Ukrainian War

Given the ongoing conflict in Ukraine, unmanned aerial vehicles (UAVs) have become a crucial element in military operations. Their application involves various methods aimed at enhancing efficiency and reducing risks for both military and civilian populations.

1. Reconnaissance and Monitoring

UAVs are used for gathering reconnaissance information and monitoring the movement of enemy forces. Micro-UAVs, in particular, can discreetly track enemy positions, providing essential data for strategic planning.

2. Tactical Strikes

Armed UAVs can be employed for precise targeting of enemy objects, such as tank convoys. This enables effective tactical strikes while minimizing the risk to friendly forces.

3. Evacuation and Medical Aid

UAVs are utilized for delivering necessary supplies and medical aid to inaccessible or hazardous areas. This is especially crucial in conflict situations where traditional delivery routes may be limited.

4. Counterintelligence

Specialized UAVs are used for detecting enemy reconnaissance sources, offering protection against hostile intelligence efforts and aiding in identifying hidden threats.

5. Electronic Warfare

UAVs can engage in electronic warfare to disrupt enemy communication signals and halt their activities.

6. Humanitarian Missions

In humanitarian crises, UAVs can be employed to deliver aid to crisis zones. They ensure swift and efficient humanitarian aid delivery without exposing human personnel to high risks.

The integration of UAVs into IoBT brings transformative synergies to modern military operations.

UAVs with IoBT capabilities become intelligent nodes in a network of interconnected devices, facilitating real-time data collection, analysis, and communication on the battlefield.

Equipped with sensors and communication modules, these UAVs not only improve situational awareness but also work seamlessly with other IoBT-enabled units such as ground robots and smart wearables worn by soldiers. This interconnected ecosystem allows militaries to respond dynamically and agilely to evolving threats, redefining strategic approaches to warfare. Nevertheless, the merger of UAV and his IoBT highlights the importance of robust cybersecurity measures.

As these technologies evolve, it becomes increasingly important to securely exchange sensitive information to ensure the effectiveness and reliability of networked systems.

The continued evolution of this symbiotic relationship between UAVs and IoBT continues to shape the future of military operations, requiring a measured approach to security challenges while providing opportunities for innovation. The integration of UAVs into military operations in Ukraine has become a key factor in the development

of strategies and tactics. They enhance operational efficiency and accuracy while reducing threats to both military and civilian populations.

Conclusions

Contexts, as evidenced by the referenced studies, reveals their diverse applications and significant contributions to modern operations. The classification methodologies and analyses provided by various researchers, such as Bilous, Glotov, and Tsimbalistova, offer comprehensive frameworks for understanding the structural features, capabilities, and purposes of UAVs.

The Ukrainian war has underscored the strategic importance of UAVs in enhancing military capabilities. The methods of application discussed, including reconnaissance, tactical strikes, evacuation, counterintelligence, electronic warfare, and humanitarian missions, showcase the versatility of UAVs in addressing various challenges on the battlefield. These methods not only contribute to military success but also play a crucial role in minimizing risks to both military personnel and civilian populations.

The ongoing conflict has prompted Ukraine to rapidly adapt to the evolving landscape of modern warfare, leveraging UAV technology for surveillance, reconnaissance, and strategic advancements. The collaborative efforts of educational, scientific, and manufacturing sectors in Ukraine have contributed to the development of indigenous UAVs, marking a significant stride in aligning with global leaders in military aircraft manufacturing.

As the use of UAVs continues to evolve, it is essential for Ukraine and other nations to stay abreast of technological advancements, address cybersecurity challenges, and navigate ethical considerations. The insights gained from the referenced studies lay the groundwork for future developments, ensuring that UAVs play a pivotal role in shaping the landscape of defense capabilities, not only in Ukraine but globally.

References

[1] Bilous, V. (2016). "Classification of Unmanned Aerial Vehicles and its Importance for Forensic Practice." Theory and Practice of Forensic Examination and Criminology, 16, 47–57.

[2] Glotov, V., Gunina, A., Telechuk, Y. (2017). "Analysis of the Possibilities of Using Unmanned Aerial Vehicles for Military Purposes." Modern Achievements in Geodetic Science and Production, Lviv, 1 (33), 139–146.

[3] Grebenikov, A., Zhuravsky, A., Myalitsa, A., et al. (2009). "Problems of Unmanned Aeronautical Complexes in Ukraine." Open Information and Computer Integrated Technologies, Kharkiv: NAKU, 42, 111–119.

[4] Minochkin, A., Sova, O., Mariliv, O., Trotsko, O. (2017). "Analysis of the Use of Unmanned Aerial Vehicles as Retransmitters of Tactical Mobile Radio Networks." Collection of Scientific Works of VITI, 1, 61–70.

[5] Nalivayko, Y., Skorik, O.M., Doska. (2009). "Features of the Tactics of the Actions of the NATO Air Force in the Suppressed Integrated Air Defense System." Navigation and Communication Management Systems, 2 (10), 124–128.
[6] Tsimbalistova, O. (2015). "Development of the Market of Unmanned Aerial Vehicle Services as the Main Direction of Innovative Progress of Modern Aviation." Economic Analysis: Sb. Sciences Works, Ternopil: Publishing and Printing Center of Ternopil National Economic University, 19(1), 116–122.
[7] Clothier, R. (2011). "UAS Classification: Key to Effective Airworthiness and Operational Regulations." In Royal Aeronautical Society Unmanned Aircraft Systems Specialist Group, UAS Classification Workshop, 24th June 2011, London, UK.
[8] Hlotov, V., Hunina, A., Kolesnichenko, V., Prokhorchuk, O., Yurkiv, M. (2018). "Development and Investigation of UAV for Aerial Surveying ISTCGCAP," No. 87, p. 48–57. [DOI: 10.23939/istcgcap2018.01.048]
[9] Meyer-Fujara, J. (n.d.). "Applications of Military and Non-Military Unmanned Aircraft Systems (UAV)." Retrieved from http://www.academia.edu/11154604/Applications_of_military_and_nonmilitary_Unmanned_Aircraft_Systems_UAV_
[10] Watts, A., Ambrosia, V., Hinkley, E. (2012). "Unmanned Aircraft Systems in Remote Sensing and Scientific Research: Classification and Considerations of Use." Remote Sens., 4, p. 1671–1692. [DOI: 10.3390/rs4061671]

НЕЙРОМЕРЕЖНИЙ ЗАСТОСУНОК КОЛОРИЗАЦІЇ ЗОБРАЖЕНЬ

Олена ФЕДУСЕНКО (к.т.н., доцент)[1]
Ірина ДОМАНЕЦЬКА (к.т.н., доцент)[2]
Ірина ІВАХНЕНКО (бакалавр, Python Developer in test)[3]

[1,2] *Київський національний університет імені Тараса Шевченка, факультет інформаційних технологій, кафедра інтелектуальних технологій, Київ, Україна*
[3] *AJAX System, Київ, Україна*
[1] fedusenko@knu.ua, [2] domanetska@knu.ua, [3] ira.ivahnenko00@gmail.com

Анотація
У роботі досліджено використання нейронних мереж, а саме, згорткової нейронної мережі, для вирішення задачі колоризації зображень. Авторами проведено аналіз процесу колоризації, запропонована архітектура застосунку, що буде складатися з трьох підсистем, розроблено програмне забезпечення та проведено аналіз його роботи.

Ключові слова
Нейромережа, колоризація зображень, згорткова мережа, нейромережний застосунок.

Вступ

Колоризація - це, по суті, процес отримання інформації про колір там, де вона відсутня. Технічно це складний процес присвоєння тривимірної колірної інформації RGB (червоний, зелений, синій) кожному пікселю з урахуванням інтенсивності напівтонового зображення у візуально прийнятний, правдоподібний спосіб. Для зменшення складності задачі в процесі колоризації використовується перетворення в зручний колірний простір "яскравість-хроматичність". YUV та CIELAB - це колірні простори, похідні від RGB. CIELAB - перцептивно однорідний колірний простір, отриманий з RGB шляхом нелінійних перетворень. Рівномірна зміна компонентів у CIELAB відповідає рівномірній зміні колірного сприйняття людини. З цієї причини спостереження двох різних кольорів в CIELAB можна апроксимувати евклідовою відстанню між відповідними точками в колірному просторі. YUV отримується з RGB шляхом лінійних перетворень [1] і не є однорідним для сприйняття. Як YUV, так і CIELAB відокремлюють компонент яскравості від інформації про колір, що дозволяє використовувати інформацію про інтенсивність і полегшує прогнозування двох інших колірних каналів. Компонент Y в YUV представляє яскравість, в той час як U і V є компонентами кольоровості. У CIELAB L - це компонент яскравості, тоді як компоненти ab несуть інформацію про колір - a представляє вісь зелений-червоний, a b - вісь синій-жовтий. Різні методи колоризації працюють з різними колірними

просторами. Хоча деякі автори аналізують вплив різних колірних просторів на процес колоризації [2], багато хто вибирає зручний для себе і розвиває метод з обраним колірним простором [3, 4].

Колоризація зображень є складною проблемою через різні умови отримання зображень, які необхідно обробляти за допомогою єдиного алгоритму. Проблема також дуже погано поставлена, оскільки два з трьох вимірів зображення відсутні; хоча семантика сцени може бути корисною в багатьох випадках, наприклад, трава зазвичай зелена, хмари зазвичай білі, а небо блакитне. Однак, такі семантичні пріоритети є дуже рідкісними для багатьох штучних та природних об'єктів, наприклад, сорочок, автомобілів, квітів тощо [5].

Зі стрімким розвитком методів глибинного навчання з'явилися різноманітні моделі розпізнавання зображень і повідомляється про їхню найсучаснішу продуктивність на поточних наборах даних. Різноманітні моделі глибинного навчання, починаючи від ранніх мереж грубої сили до нещодавно ретельно розроблених генеративних змагальних мереж (GAN) (наприклад, [6]), були успішно використані для вирішення проблеми колоризації. Ці мережі розфарбовування відрізняються за багатьма основними параметрами, включаючи архітектуру мережі, глибину мережі, функції втрат, стратегії навчання тощо.

Метою дослідження є розробка нейромережевого застосунку для колоризації зображень

Результати дослідження

Метою колоризації є оцінка кольорів RGB напівтонового зображення, яке зазвичай знімалося кольоровими камерами до того, як кольорові камери стали широко доступними, а технологічний прогрес був обмеженим. Отже, цей процес є скоріше формою покращення зображення, ніж його відновлення. Іншим застосуванням колоризації зображень є відновлення кольорових зображень після їх перетворення у відтінки сірого або Y-канал кольорового простору YUV, наприклад, для економії місця на носіях інформації або пропускної здатності каналу зв'язку. Тому в даному випадку тривіальна формула може бути записана як формула (1):

$$I_g = \Phi(I_{rgb}) \tag{1}$$

де Ф(-) - функція, яка перетворює RGB зображення в зображення у відтінках сірого , наприклад, формула (2):

$$I_g = 0.2989 \cdot I_r + 0.5870 \cdot I_g + 0.1140 \cdot I_b \tag{2}$$

Як правило, методи колоризації спрямовані на відновлення кольору в просторі YUV, де модель повинна прогнозувати тільки два канали, тобто U і V - замість трьох каналів в RGB [7].

Для реалізації нейромережного застосунку будемо використовувати розфарбування зображень, який є методом глибокого навчання, що використовує штучні нейронні мережі для автоматичного розфарбовування вхідного зображення у відтінках сірого у природні кольори. Це відбувається шляхом вивчення відповідності між інтенсивністю рівня сірого вхідного зображення та значеннями RGB вихідного зображення.

Процес розфарбовування зображень складається з чотирьох основних етапів: попередня обробка зображень, виділення ознак, розфарбування, пост-обробка.

Процес колоризації зображень з використанням нейромережного застосунку наведено на рис. 1.

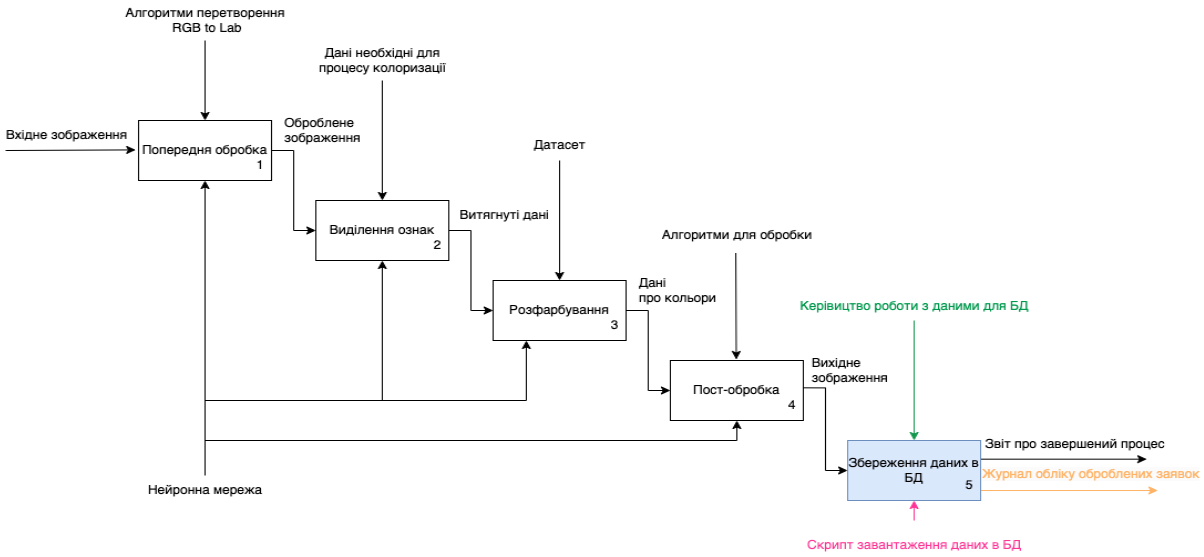


Рис. 1. Процес колоризації зображень з використанням нейромережного застосунку

Даний застосунок буде складатися з декількох підсистем, а саме:

1. Підсистема взаємодії з користувачем - це основна сторінка системи, яка містить модуль завантаження зображень, модуль отримання вихідного зображення та модуль збереження даних в базу даних.
2. Підсистема роботи з зображеннями складається з модуля попередньої обробки, модуля колоризації зображень та модуля після обробки.
3. Особистий кабінет користувача містить модуль інформації про користувача та модуль поточних проектів користувача, які з’єднуються з базою даних.

Для колоризації зображень у застосунку було прийнято рішення використовувати згорткову нейрону мережу(CNN) оскільки її використання дозволить зменшити кількість параметрів які потрібно тренувати, без шкоди для продуктивності. Згорткова нейронна мережа – це нейронна мережа, яка

використовує шар згортки і шар об'єднання. Згортковий шар згортається в меншу область для вилучення ознак, в той час як шар об'єднання вибирає дані з найбільшим значенням в межах області. Вони вимагають меншої попередньої обробки в порівнянні з іншими алгоритмами класифікації і здатні навчатися фільтрам і характеристикам [8].

Робота розробленого нейромережного застосунку для колорізації зображень наведено на рис.2.

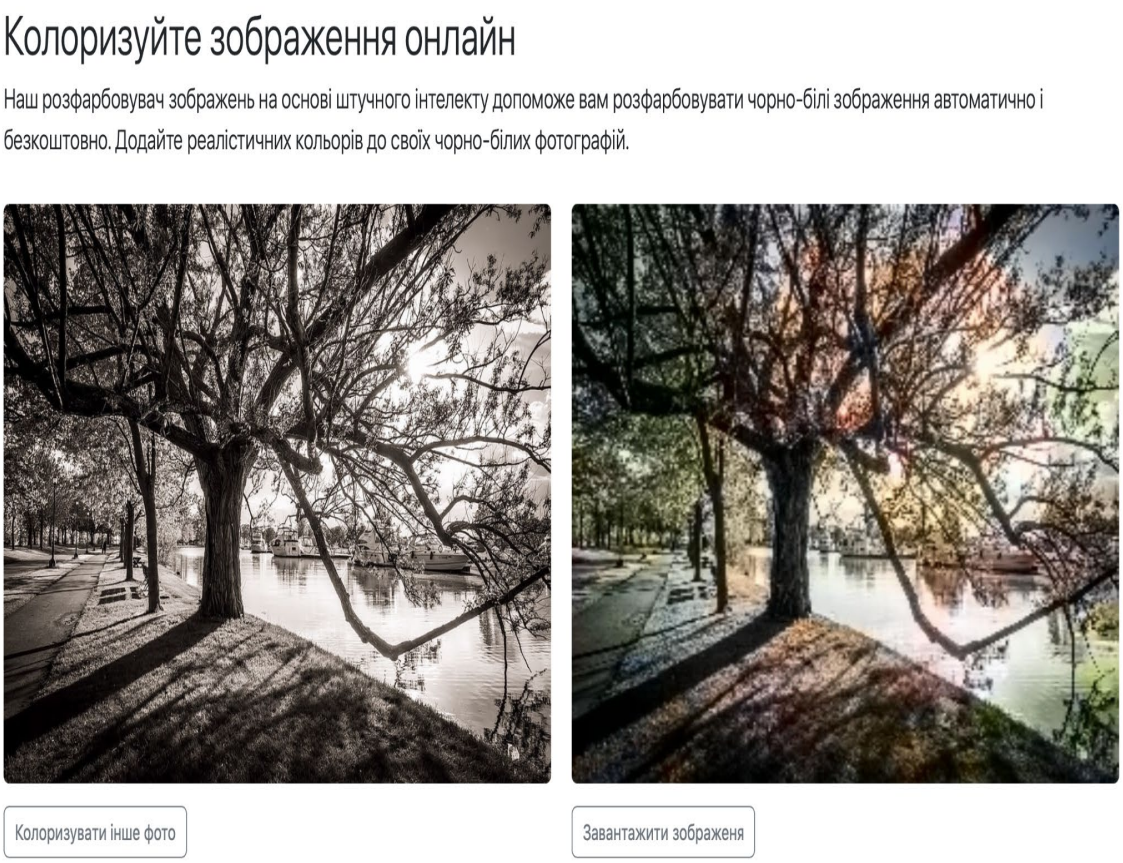


Рис. 2. Приклад роботи нейромережного застосунку

Проведемо аналіз роботи розробленого нейромережного застосунку для колоризації зображень за наступними критеріями: точність, швидкість, загальна стабільність (табл. 1).

Таблиця 1

Результати роботи нейронної мережі

Критерій	Результат
Точність	Найкращі результати колоризації фотографій зафіксовані у природних сценах, зокрема неба, моря та трави, оскільки вони характеризуються чіткими кольорами та текстурами.

	Колоризація фотографій людей викликана складністю передачі правильних відтінків шкіри та деталей обличчя. Колоризація фотографій тварин була успішною, хоча складніші або незвичайні малюнки можуть потребувати додаткових зусиль для точного відтворення кольорів.
Швидкість	До 100 КБ - 2 с, до 500 КБ - 3 с, до 1 МБ - 7 с, до 6 МБ - 10 с.
Загальна стабільність	Під час повторних запусків отримуємо однакові результати.

Отже, результати роботи системи є залежними від характеру зображення та його складності. Більш складні фото, котрі мають велику кількість дрібних деталей, можуть потребувати додаткової обробки або налаштувань системи для досягнення більш точних результатів.

Висновки

У роботі було розглянуто проблему колоризації зображень за допомогою нейромереж та розроблено застосунок для колоризації зображень, який використовує згорткову нейрону мережу. Отримані за допомогою застосунку результати колоризації показали, що найкращі результати були досягнуті на природних сценах, проте колоризація фотографій людей не була настільки точною, зокрема є проблеми при розфарбуванні обличчя. Під час тестування системи було виявлено, що складні зображення з багатьма дрібними деталями можуть потребувати додаткової обробки або налаштувань для досягнення кращих результатів.

Незважаючи на ці недоліки колоризація зображень за допомогою нейромереж має перспективи та потенціал для розвитку.

Література

[1] Y. Di, X. Zhu, X. Jin, Q. Dou, W. Zhou, and Q. Duan, «Color- UNet++: A resolution for colorization of grayscale images using improved UNet++», Multimedia Tools Appl., Mar. 2021, p. 1–20.

[2] S.Huang, X.Jin, Q.Jiang, J.Li, S.-J.Lee, P.Wang, andS.Yao, «A fully- automatic image colorization scheme using improved CycleGAN with skip connections», Multimedia Tools Appl., May 2021.

[3] J.-W. Su, H.-K. Chu, and J.-B. Huang, «Instance-aware image colorization», in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2020, p. 7965–7974.

[4] P. Vitoria, L. Raad, and C. Ballester, «ChromaGAN: Adversarial picture colorization with semantic class distribution» in Proc. IEEE Winter Conf. Appl. Comput. Vis. (WACV), Mar. 2020, p. 2445–2454.

[5] Ivana Žeger, Sonja Grgic, Josip Vuković, Gordan Šišul, «Grayscale Image Colorization Methods: Overview and Evaluation», August 2021.
[6] S. Yoo, H. Bahng, S. Chung, J. Lee, J. Chang, and J. Choo, «Coloring with limited data: Few-shot colorization via memory augmented networks», in IEEE Conference on Computer Vision and Pattern Recognition, 2019, p. 11283–11292.
[7] Saeed Anwar, Muhammad Tahir, Chongyi Li, Ajmal Mian, Fahad Shahbaz Khan, Abdul Wahab Muzaffar, «Image Colorization: A Survey and Dataset». Accessed: 2021. [Online]. Available: *https://ieeexplore.ieee.org/document/9512069*.
[8] A. Khan, A. Sohail, U. Zahoora, and A. S. Qureshi, «A survey of the recent architectures of deep convolutional neural networks». Accessed: 2019. [Online]. Available: *http://arxiv.org/abs/1901.06032*.

АНАЛІЗ НАПРЯМКІВ РОЗВИТКУ ТА ПРОБЛЕМ ЗАХИСТУ IoT

Дмитро ТАРАСЮК (асистент)[1]
Володимир ВИШНЯКОВ (кандидат технічних наук, доцент)[2]

Київський національний університет будівництва і архітектури, факультет автоматизації і інформаційних технологій, кафедра кібербезпеки та комп'ютерної інженерії, Київ, Україна
[1] D.Tarasiuk+TTSIIT@membrama.com, [2] volodymyr.vyshniakov@gmail.com

Анотація
Нейронні мережі в інфраструктурі Інтернету речей (IoT) розширяють її можливості, ускладнюють та персоніфікують її поведінку. Такі системи IoT інкапсулюють багато чутливої приватної інформації про користувачів, яка потребує захисту. Наявні стандарти ще дозволяють нехтувати безпекою. Наводиться приклад побудови «розумного» брандмауера для компенсації безпекових ризиків.

Ключові слова
Інтернет речей, нейронна мережа, туманні обчислення, «розумний» будинок, «розумний завод», «розумне місто», безпека, «розумний» брандмауер.

Abstract
Neural networks in the Internet of Things (IoT) infrastructure extend its capabilities, complicate and personalize its behavior. Such IoT systems encapsulate a lot of sensitive private information about users that needs to be protected. Existing standards will still refuse to neglect safety. An example of building a "smart" firewall to compensate for security risks is given.

Keywords
Internet of the things, neural network, fog computation, smart house, smart factory, smart city, security, “smart firewall”.

Постановка проблеми

Інтернет речей – це сфера, яка однією з перших за своєю побудовою та можливостями включає в себе досягнення штучного інтелекту. Очікується, що Інтернет речей призведе до Четвертої промислової революції та докорінно змінить багато галузей економіки та побут людей у найближчі 10-20 років. Не помічати перспектив розвитку Інтернету речей неможливо. В інфраструктуру Інтернету речей входить множина автентифікованих пристроїв, що поєднані у мережу. На периметрі Інтернету речей знаходиться Агент. В найпростішому випадку це може бути веб-сторінка, на якій зібрані всі покази сенсорів та віджети для керування виконавчими пристроями.

Ось деякі тенденції розвитку Інтернету речей, які можна передбачити вже зараз:

- Подальше стрімке зростання кількості підключених до мережі пристроїв та обсягів даних, що генеруються. Прогнозується десятки мільярдів IoT-пристроїв вже до 2025 року [1].
- Поширення концепції «розумного середовища» - коли Інтернет речей інтегрується з інфраструктурою міст, будівель, заводів.
- Мережі 5G, хмарні та туманні обчислення стануть основою для масштабних застосувань Інтернету речей.
- Штучний інтелект буде все активніше застосовуватися для аналізу даних і прийняття рішень в IoT. Для їх підтримки з'являтимуться спеціалізовані одноплатні мікрокомп'ютери[2] та технології інтеграції роботи нейронних мереж в існуючий обчислювальний парк (Raspberry Pi, смартфони)[3].
- Аналогові обчислення[4] при перемноженні тензорів нейронних в комірках пам'яті[5] значно зменшать енергоспоживання та пришвидшать роботу нейронних мереж.
- Блокчейн дозволить покращити безпеку та довіру до даних і пристроїв IoT шляхом децентралізованого контролю.

Впровадження IoT має не лише позитивний вплив, але й пов'язано з виникненням ризиків кібератак з витоком конфіденційних даних. Порушник може дізнатись, де знаходиться власник, його наміри, розклад дій, залежності, стан здоров'я. Також може виникати залежність людини від роботи пристроїв IoT. Оскільки у системі IoT зберігається багато інформації, яка має захищатись від витоку за периметр Інтернету речей. Ці проблеми потребують вирішення, як на технічному, так і на законодавчому рівні.

Мета доповіді

Метою доповіді є надання пропозицій щодо розв'язання перелічених проблем за рахунок впровадження технічних рішень, які дозволяють забезпечити захист системи IoT від кібератак.

Огляд та аналіз нормативних документів та стандартів щодо IoT

Для підтримки технологій Інтернету речей в галузі будівництва розроблені наступні спеціальні стандарти та концепції «розумних будівель»:

- ISO/IEC 30141 «Інтернет речей». Стандартизація та впровадження «розумне місто».
- ISO/IEC 21823-1 «Інтернет речей». Інтероперабельність IoT систем. Частина 1: Рамкова структура.
- IEEE 1934-2018. Стандарт для прийняття еталонної архітектури OpenFog для «туманних обчислень». Такі обчислення забезпечують локальну обробку та аналіз даних, фільтрацію трафіку, дозволяють істотно зменшити обсяги

даних, що передаються на централізовану обробку, забезпечують низьку затримку для критичних IoT застосувань.

- IETF STD RFC 7452. Архітектурні принципи для протоколів і форматів даних «розумних об'єктів» Інтернету речей.
- IEEE P2413 Стандарт архітектурної основи Інтернету речей. Визначає архітектурну структуру для Інтернету речей (IoT), включаючи описи різних доменів IoT, визначення абстракцій домену IoT та ідентифікацію спільного між різними доменами IoT. Надається еталонна модель, яка визначає взаємозв'язки між різними вертикалями IoT і загальними елементами архітектури. Надає схему для абстракції даних і «четверної» довіри до якості, що включає захист та безпеку. Забезпечує еталонну архітектуру, яка базується на еталонній моделі. Вона охоплює визначення основних архітектурних будівельних блоків та їх здатність інтегруватися в багаторівневі системи.
- ETSI TS 103 645. Кібербезпека для споживчого Інтернету речей: Базові вимоги.

Ці стандарти визначають вимоги, архітектуру, протоколи та API для інтеграції систем Інтернету речей в інфраструктуру розумних будівель, міст, заводів, тощо. Вони спрямовані на забезпечення сумісності, безпеки та надійного зв'язку між IoT пристроями.

Наведені стандарти закладають важливу основу для безпеки рішень Інтернету речей, але не можна сказати, що цього достатньо. Для комплексного забезпечення безпеки потрібен системний багатошаровий підхід, у відповідності до ризиків та критичності застосувань. Цей підхід має бути не тільки технічний, а й організаційний, в тому числі потрібно визначати вимоги до обслуговування, модернізації, ремонту, інтеграції зі штучним інтелектом, утилізації, копіювання, мінімальний рівень дублювання критичних підсистем, умови доступу правоохоронних органів, дозволені засоби захисту від втручань.

Отже, сучасні та майбутні стандарти закладають основу, але безпека – це комплексна предметна область, яка потребує особливої постійної уваги.

Пропозиції щодо впровадження розумного брандмауера

Використовуючи формалізований опис IoT у вигляді системи рівнянь може бути задана математичну модель системи. Це дозволяє аналізувати її роботу і побудувати брандмауер обміну даними в інфраструктурі Інтернету речей, скориставшись наступним підходом:

1. Для кожного пристрою визначаємо нормований обсяг даних, які він може передавати у вигляді множини (N_1, N_2, ..., N_n).
2. Вводимо змінні, що відповідають відхиленню трафіку від норми для усіх пристроїв:

$D_1 = P_1 - N_1$
$D_2 = P_2 - N_2$
...

3. Формулюємо правило блокування аномальних підключень у наступному вигляді:

Якщо Di > МАКС_ВІДХИЛЕННЯ, то блокувати P_i,
де МАКС_ВІДХИЛЕННЯ — це граничне значення.

Такий підхід дозволяє контролювати обмін даними між пристроями і реагувати на спроби несанкціонованого доступу на основі математичної моделі.

Математична модель може бути застосована для автоматичного машинного (до)навчання нейромережі або працювати одночасно з нею в симбіозі за наступним сценарієм:

1. Збираються дані про нормальну поведінку трафіку в мережі (розмір та особливості пакетів, IP адреси, протоколи, час з'єднань, режим роботи, розпізнані особи).
2. Отримані дані використовуються для (до)навчання моделі (наприклад, нейронної мережі або моделі, що базована на опорних векторах або на дереві (лісі) рішень. Перевагу слід надати моделі, яка дозволяє краще пояснити свій вибір.
3. Модель з часом навчається відрізняти нормальний трафік від аномального у разі атак зловмисників.
4. Після навчання модель вбудовується безпосередньо на маршрутизатори чи інші пристрої комп'ютерної мережі.
5. Модель в режимі реального часу аналізує мережевий трафік і блокує потенційно небезпечні запити та з'єднання, що відхиляються від норми.
6. Така система надає можливість побудувати ефективний захист від кібератак на рівні мережевої взаємодії пристроїв IoT.

Висновки

Впровадження систем IoT дозволяє вирішувати складні задачі по-новому, але водночас з’являються проблеми, що пов’язані з безпекою, бо зловмисне втручання в роботу систем IoT має незрівнянно більший негативний вплив в порівнянні з розрізненою множиною окремих зловживань.

Існуючі стандарти у галузі IoT визначають вимоги, архітектуру, протоколи та API для інтеграції систем Інтернету речей в інфраструктуру розумних будівель, підприємств та міст, але безпека – це комплексна предметна область, яка потребує особливої постійної уваги.

Запропоновані у доповіді технічні рішення дозволяють забезпечити захист систем IoT від кібератак за рахунок впровадження розумного брандмауера з використанням нейромережі та елементів штучного інтелекту.

Література

[1] Романов Роман. Звіт: кількість підключених пристроїв IoT зросла на 18% до 14,4 мільярдів по всьому світу. 20 травня 2022, 09:20. URL: https://internetua.com/zvit-kilkist-pidkluacsenih-pristroyiv-iot-zrosla-na-18-do-14-4-milyardiv-po-vsomu-svitu.
[2] BeagleBone® AI-64. URL: https://www.beagleboard.org/boards/beaglebone-ai-64.
[3] Open Neural Network Exchange. URL: https://onnx.ai/.
[4] Analog Computing. URL: https://mythic.ai/technology/analog-computing/.
[5] Compute-In-Memory. URL: https://mythic.ai/technology/compute-in-memory/.

ПРИНЦИПИ СИСТЕМНОСТІ УПРАВЛІННЯ РИЗИКАМИ СКЛАДНИХ ІНФОРМАЦІЙНИХ СИСТЕМ З ЗАСТОСУВАННЯМ IoT

Ольга ІЗМАЙЛОВА (к.т.н., доцент)[1]
Ганна КРАСОВСЬКА (к.т.н., доцент)[2]

[1] Київський національний університете будівництва і архітектури, факультет автоматизації і інформаційних технологій, кафедра кібербезпеки та комп'ютерної інженерії, Київ, Україна
[2] Київський національний університет імені Тараса Шевченка, факультет інформаційних технологій, кафедра інтелектуальних технологій, Київ, Україна
[1] izmailova.ov@knuba.edu.ua, [2] hanna.krasovska@knu.ua

Анотація
У роботі проаналізовано концептуальні основи побудови систем управління ризиками складних інформаційних систем з застосуванням IoT на основі системного підходу. Результати досліджень представлені у вигляді сукупності принципів системності управління ризиками.

Ключові слова
Управління ризиками, принципи системності, системи інтернету речей, цифрова трансформація компанії, архітектура системи.

Вступ

Безпека інтернету речей має свою специфіку і зазвичай стає головним пріоритетом в інформаційних системах. Досвід використання свідчить, коли до вже традиційної інформаційної системи додають компоненти IoT, то поряд зі значним поширення можливостей та послуг, вони беруть на себе роль потенційно критично вразливої системи. В цих умовах на різних управлінських рівнях роботи компанії з застосування складних систем з використанням IoT зростає актуальність розв'язання проблеми удосконалення системи управління ризиками інформаційної безпеки з системною трансформацією існуючих наробок в теорії і практиці функціонування сучасних компаній універсальних ефективних систем управління ризиками [1-5] з врахуванням особливостей вимог до систем такого класу та специфіки систем захисту IoT.

Метою дослідження є аналіз концептуальних основ побудови систем управління ризиками складних інформаційних систем з застосуванням IoT на основі системного підходу у вигляді сукупності принципів його реалізації.

Результати дослідження.

Складні системи з застосуванням IoT формують новий додатковий світ віртуальної реальності функціонування інформаційної системи і разом з тим надають множину нових загроз, що пов'язані як з окремими пристроями, і платформами їх функціонування, засобами трансформації, переробки та передачі даних для реалізації процесів інформаційної технології. Складні системи з використанням IoT різноманітні з точки зору вимог профілю різних предметних областей, сутності та цільових установок функціонування, але мають загальні типові риси, з врахуванням яких можна проаналізувати доцільність та ефективність, визначити загальні шляхи удосконалення систем управління ризиками на основі системного підходу. Системний підхід управління ризиками передбачає необхідність врахування усіх взаємозв'язаних взаємодіючих та змінних у часі різноаспектних компонентів архітектури системи, умов та факторів для всіх режимах функціонування, на всіх етапах життєвого циклу з врахуванням зв'язку системи та об'єкту захисту з зовнішнім середовищем. Системний підхід у дослідженні управління можна представити в сукупності принципів, яким необхідно слідувати і які відображають як зміст, так і особливість підходу до управління ризиками складних систем з застосуванням IoT.

Принцип системно-цільового підходу розробки системи. Це основний принцип системного підходу, що передбачає встановлення головної (глобальної) цілі управління кібербезпекою компанії, що полягає в найточнішому виявлення можливих відхилень від запланованих результатів та управління цими відхиленнями з метою підвищення ефективності роботи компанії. Цей принцип передбачає:

- визначення та змістовне тлумачення глобальної цілі управління кібербезпекою компанії;
- оцінку основних факторів, що негативно впливають на ключові ризики компанії та досягнення глобальної цілі кібербезпеки (загрози, активи, уразливості, цінності активів);
- виявлення та аналіз часткових цілей та засобів забезпечення кібербезпеки системи для оптимізації досягнення поставленою перед нею головної (глобальної) цілі;
- домінування глобальної цілі кібербезпеки системи в порівнянні з локальними потребами та можливостями захисту окремих її компонентів (реалізація окремих несистемних заходів, спрямованих на зниження негативного впливу окремого фактору ризику, не дозволяє отримати системну оптимізацію);
- ефективність управління ризиком з урахування внутрішніх і зовнішніх взаємозв'язків компонентів функціонування системи на різних рівнях її побудови та захисту – рівень мережі, рівень операційної системи, рівень баз даних та знань, рівень застосувань (програмні модулі та конкретні апаратні засоби, персонал)., під впливом яких здійснюється функціонування компанії. Особлива

увага приділяється апаратним засобам IoT, що працюють з великими обсягами даних, які збираються з відповідних пристроїв-датчиків RFID та мобільних пристроїв;

- зв'язок управління ризиками із стратегічними цілями компанії управління ризиками, що є невід'ємною частиною процесу прийняття рішень на всіх рівнях її функціонування.

Принцип оптимальності. Даний принцип підкреслює можливість розбіжності локальних оптимумів окремих цілей оптимізації ризиків або окремих активів системи з глобальною ціллю системи. Тому він вказує на необхідність в цілях досягнення глобальних цільових результатів приймати рішення і вести розробки з удосконалення систем не тільки на основі даних аналізу дерева цілей , але й синтезу можливих засобів оптимізації кіберзахисту.

Принцип врахування системних вимог цифрової трансформації бізнесу компанії. Цифрова трансформація зараз є однією з найгарячіших бізнес-тем сучасної компанії. Складні системи з застосуванням IoT є вирішальним вагомим фактором цифрової трансформації компанії. Управління ризиками в умовах цифрової трансформації компанії повинно базуватися на аналізі і синтезі рішень, їх оптимізації на різних рівнях цифрової трансформації. Так, в роботі [6] запропоновані в якості базових три рівні: організація, бізнес-процес, інформаційна технологія (рис.1).

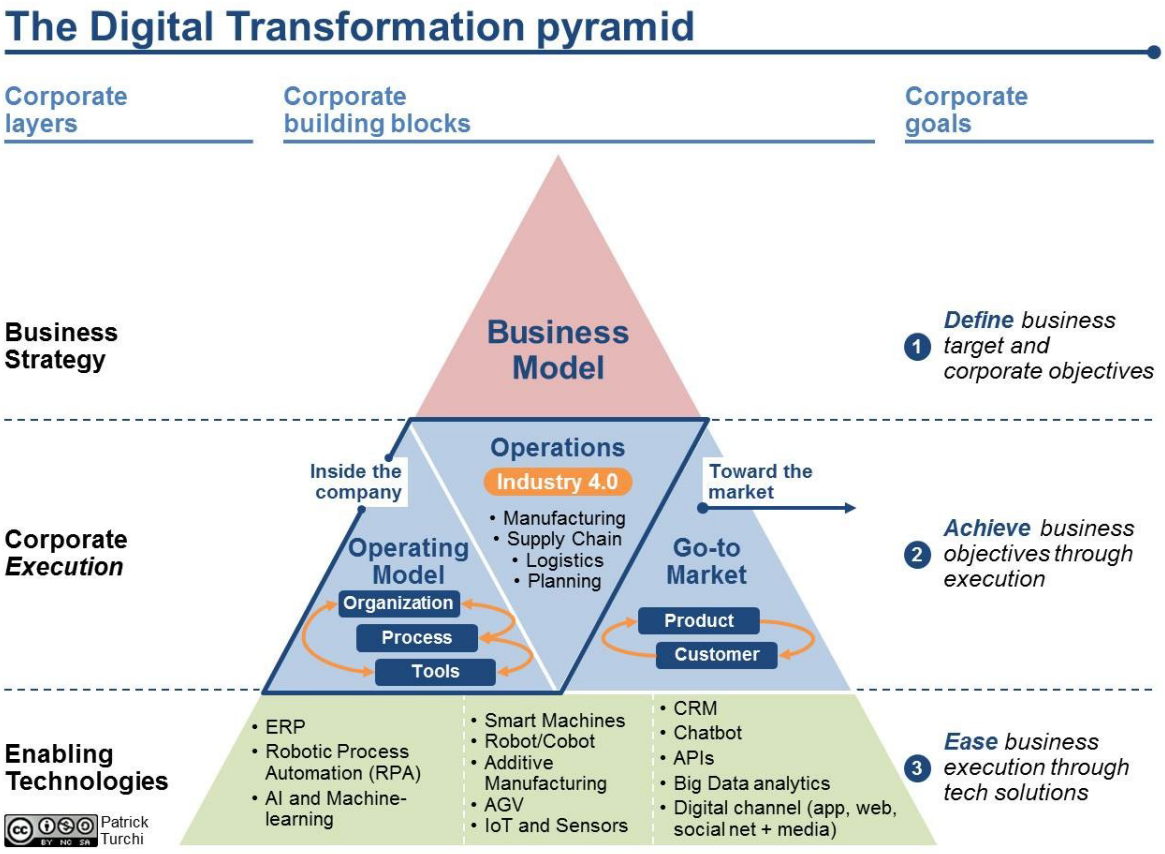


Рис.1. Піраміда цифрової трансформації бізнес-компанії [6]

Управління ризиками ведеться на рівнях організації, бізнес-процесів та інформаційних систем, при цьому слід забезпечувати взаємозв'язок та обмін інформацією між цими рівнями з метою безперервного підвищення ефективності здійснюваних дій На верхньому рівні (рівні організації) здійснюється ухвалення рішень щодо визначення ризиків, що безпосередньо впливає на процеси, що ведуть на нижчих рівнях (бізнес-процесів та інформаційних систем).

Принцип систематизації інформаційних активів, бізнес-процесів, процесів управління, пов'язаних з обробкою ризиків. Забезпечення у спеціалістів з кібербезпеки **системного уявлення про предметну область розробки** за рахунок аналізу різноаспектних, зв'язаних у цілісне представлення моделей функціонування інформаційної системи, що проектується або функціонує, їх призначення та особливості функціонування з метою визначення об'єктів захисту, типів можливих загроз та засобів захисту. Пропонується **система моделей архітектури системи**, яка відображає структурний аспект функціонування. Структурний аспект передбачає побудову **об'єктної структури**, що відбиває склад взаємодіючих в процесах матеріальних та інформаційних об'єктів предметної області, в тому числі системи IoT; **функціональної структури**, що відбиває взаємозв'язок функцій (дій) щодо перетворення об'єктів в процесах, в тому числі дій системи IoT, що пов'язані зі збором, аналізом, обробкою та передачею інформації з використанням бази даних та відповідного програмного забезпечення, додатків чи технічних засобів; **структури управління**, що відображає події та бізнес-правила, які впливають на виконання процесів; **організаційної структури**, що відбиває взаємодію організаційних одиниць компанії і персоналу в процесах, визначає роль користувача; **технічної структури**, яка описує топологію розташування і способи комунікації комплексу технічних засобів IoT, в тому числі система датчиків та пристроїв інтернету речей, основ передачі даних в їх мережевій структурі.

Завершальним етапом моделювання є побудова **процесових моделей**. Їх значення полягає в відображенні функцій, що отримані на етапі структурного моделювання, в модулі інформаційних систем.

Принцип системного уявлення структури системи IoT. Забезпечення у спеціалістів з кібербезпеки **системного уявлення про структуру системи IoT** як складової частини з метою визначення особливостей активів IoT як об'єктів захисту, типів можливих загроз та засобів захисту, притаманних системі IoT. Основи опису структури системи IoT є моделі її архітектури, що як правило, включають граничну область (рис.2) [7]:

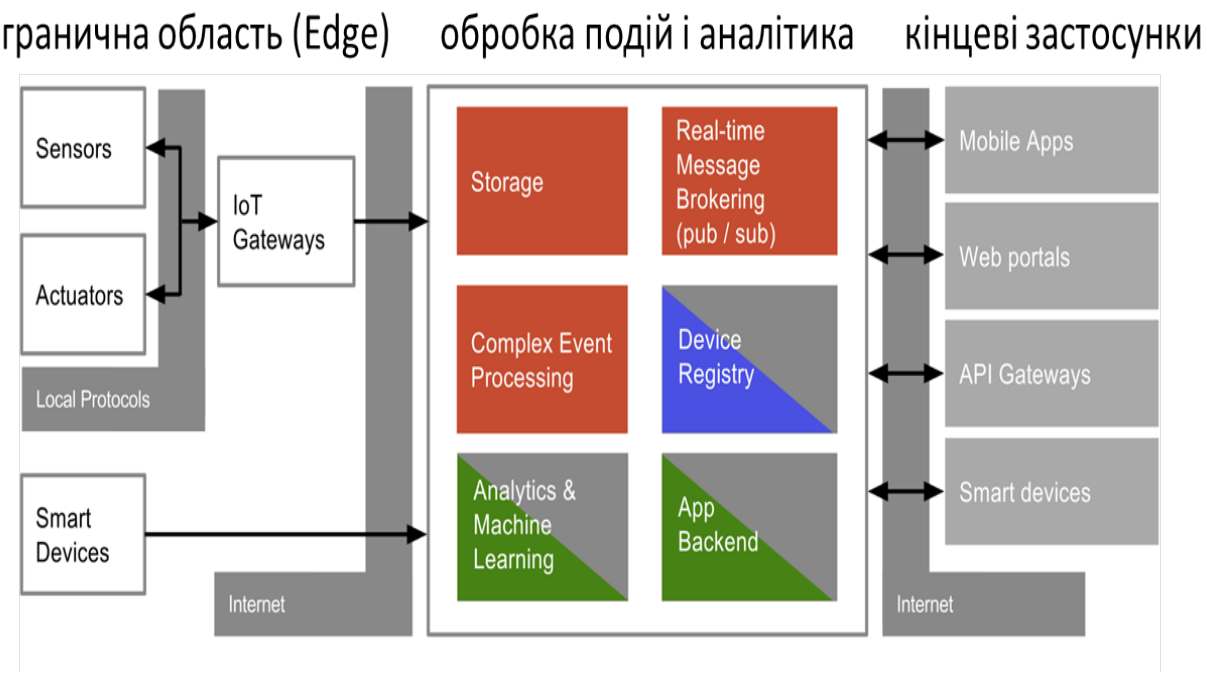


Рис. 2. Моделі архітектури системи IoT [7]

Взаємодія інформаційної системи з IoT відбувається через датчики (sensors) та виконавчі механізми (Actuators). Ці датчики разом з усією інфраструктурою для інтеграції з рівнем обробки подій, як правило через мережу Internet, формують так звану граничну область (**Edge**). Дані, що поступають з граничної області зберігаються і обробляються відповідно до задачі (рівень обробки подій і аналітики, **event processing**, **Platform**). На цьому рівні події (дані) зберігаються (storage), обробляються (Event Processing), перенаправляються для обробки в процесах складної системи (Real-Time Message Brokering, Stream Processing). Додатково на цьому рівні відбувається адміністрування та керування пристроями з граничної області (Device Registry, Edge Device Management). Отримання результатів, контроль, віддалене керування та адміністрування системи проводиться через кінцеві застосунки.

Принцип ефективності. *Означає необхідність пошуку раціонального співвідношення між витратами на створення системи захисту та цільовими ефектами захисту, досягнутими завдяки її функціонуванню.*

Принцип безперервності передбачає, що аналіз ризику і пошук методів зниження його негативних наслідків повинен вестися постійно з врахування відповідних установок політики безпеки компанії, існуючих ситуаційних умов прийняття рішень, правил та протоколів її реалізації. Процес управління ризиком повинен бути включений в єдиний контур управління роботи компанії.

Принцип діагностики критичних параметрів ризику. Управління підприємством повинне спиратися на науково обґрунтоване прогнозування можливих наслідків і виявлення потенційно найбільш серйозних джерел і умов ризику та оцінки якісних та кількісних показників ризику відповідно зі встановленою

шкалою оцінювання та сигналізацією про появу їх критичних значень – сфери неприпустимого та критичного ризику.

Принцип багатоваріантності концентрує увагу на забезпеченні на кожному етапі управління ризиком пошуку і аналізу альтернатив можливих рішень, що найбільш ефективно відповідають ситуаційним умовам управління з метою ефективного досягнення поставлених цілей. Принцип реалізується за рахунок багатоваріантності моделей та методів оцінки ризиків та вибору заходів їх зниження з метою системної цілеспрямованої оптимізації рішень.

Принцип врахування неструктурованої та слабко структурованої проблеми прийняття рішень. Управління ризиками, з одного боку, повинно забезпечити системність оцінювання з врахуванням різноаспектності вимог до міри формалізації процесів та удосконалення математичного апарату реалізації, підвищення рівня достовірності та доступності реалізації та, з іншого боку, врахування незбіжності реальних умов неструктурованої проблеми прийняття рішень та концептуальної невизначеності. Неструктурована проблема прийняття рішень управління ризиками характеризується тим, що неможливо та в багатьох випадках недоцільно застосування тільки аналітичних кількісних розрахунків. В цих умовах врахування та забезпечення комп'ютерного інструментарію використання досвіду та знань «людини» дозволяють удосконалювати прийняті рішення та результати їх реалізації.

Принцип багатоаспектності оцінки цінності об'єктів захисту. Принцип концентрує увагу на необхідності відходити від стандарту врахування тільки фінансових збитків при реалізації загроз порушення конфіденційності, цілісності та доступності даних, і потребує удосконалення результатів оцінювання на основі структуризації оцінок втрат за багатьма критеріями та врахування їх порівняльного пріоритету.

Висновки

Роль та значущість сформульованих принципів підтверджується активною діяльністю міжнародних організацій по стандартизації в цьому напрямі, розробкою та накопиченням в практиці функціонування сучасних компаній універсальних ефективних систем управління ризиками, в тому числі в складних системах з застосуванням IoT [1-6]. Це дозволяє зробити висновок про актуальність подальшого розвитку можливостей систем управління ризику систем такого класу на основі розвитку та удосконалення людино-машинного інструментарію реалізації етапів управління ризиками в концепції реалізації принципів побудови визначених систем.

Література

[1] Gross G. Key Big Data Security Issues [Electronic resource] / G. Gross// Alien Vault. – 2016. – Access: https://www.alienvault.com/blogs/securityessentials/9-key-big-data-security-issues.
[2] NIST Special Publication 800-37, Revision 2. Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy, 2018.
[3] Потій О.В., Горбенко Ю.І., Замула О.А., Ісірова К.В.Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки. Радіотехніка. 2021. Вип. 206 , с.5- 24. doi:10.30837/rt.2021.3.206.01.
[4] Common Vulnerability Scoring System version 3.1: Specification Document CVSS Version 3.1 Release https://www.first.org/cvss/v3.1/specification-document for CVSS.
[5] Izmailova, H. Krasovska, K. Krasovska & V. Zaslavskyi Assessing the Variety of Expected Losses upon the Materialisation of Threatsto Banking Information Systems. *Information & Security: An International Journal*, vol.45, p. 89-118, 2020.Available:https://isij.eu/article/assessing-variety-expected-losses-upon-materialisation-threats-banking-information-systems Accessed on: 15.12.2020 https://doi.org/10.11610/isij.4506.
[6] Turchi, P., 2018. The Digital Transformation Pyramid: A Business-driven Approach for Corporate Initiatives.[Online] Available from: https://www.linkedin.com/pulse/digital-transformation-pyramid-business-driven-approach-turchi [Accessed 03/02/2021].
[7] Стратегії цифровізації підприємств. Технології індустрії 4.0. [On-line] http://edu.asu.in.ua/mod/book/view.php?id=112&chapterid=230.

ПОНЯТТЯ І МІСЦЕ SMART SCHOOL В КОНЦЕПЦІЇ ІНФРАСТРУКТУРИ SMART CITY

Леся КОЗУБЦОВА (к.т.н, доцент, завідувач кафедри)[1]
Ігорь КОЗУБЦОВ (доктор пед. наук, к.т.н, старший науковий співробітник)[2]

[1] *Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, кафедра математики та фізики, Київ Україна*
[2] *Луцький національний технічний університет України, кафедра комп'ютерних наук, Луцьк, Україна*
[1] lesia.kozubtsova@viti.edu.ua, [2] I.kozubtsov@lntu.edu.ua

Анотація
Концепція Smart School - гнучкість, що передбачає наявність великої кількості джерел, максимальна різноманітність мультимедіа, здатність швидко і просто налаштовується під рівень і потреби учня. В умовах постійного зростання і оновлення знань безперервний розвиток компетенцій протягом всієї кар'єри стає найбільш актуальним в системі сучасної освіти. Для розвитку освіти вже недостатньо впливу людського капіталу. Необхідно змінювати саму освітнє середовище, не просто нарощувати обсяги утворення трудових ресурсів, має якісно змінитися сам зміст освіти, його методи, інструменти та середовища, необхідний перехід до SMART-утворення.

Abstract
The Smart School concept is flexible, which implies the availability of a large number of sources, the maximum variety of multimedia, and the ability to quickly and easily adjust to the level and needs of the student. In the context of constant growth and updating of knowledge, the continuous development of competencies throughout a career is becoming the most relevant in the modern education system. The influence of human capital is no longer enough for the development of education. It is necessary to change the educational environment itself, not just to increase the volume of labor resources, the content of education itself, its methods, tools and environments must change qualitatively, and a transition to SMART education is needed.

Вступ

Розумне місто – це набір певних інформаційних та цифрових технологій, які роблять життя легшим, дешевшим і комфортнішим у сучасних містах, що стикаються з багатьма викликами. Цьому сприяла ухвала Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації [1].

Як відомо розумне місто (Smart city) – це місто, яке використовує сучасні технології для покращення якості життя [2]. Технології розумного міста інтегруються у відповідні структури для підвищення якості надання послуг, зменшення витрат і споживання ресурсів, покращення комунікації та взаєморозуміння з населенням.

Експерти з архітектури [2] виділили наступні характеристики технології, пов'язані з «Smart City»:

це має бути прикладна електронна або цифрова технологія, яка працює на місто;

розробка може використовувати інформаційно-цифрові технології для трансформації житлових та робочих умов у регіоні;

технологія може бути інтегрованою для покращення роботи місцевої влади;

громада та міські спеціалісти можуть використовувати ці технології за територіальною ознакою для здобуття нових знань та початку інноваційного руху.

Але розумні міста зараз називають також мегапроектами, що створюють нові міста з нуля. Щоправда, жоден з цих інвестиційних проектів ще не реалізований повністю, але вони є результатом великих міжурядових угод. Людська цивілізація намагається вирішити проблеми масової урбанізації - тренду минулого століття - спільними зусиллями та ресурсами.

Напрацювання розумного міста можуть бути використані в багатьох сферах управління містом, таких як транспорт, електронне урядування, енергетика, охорона здоров'я, будівництво та громадське життя та закладах освіти в тому числі в школах. У кожній з цих сфер інноваційні розробки можуть бути застосовані для скорочення витрат і оптимізації використання ресурсів.

Предметом нашого дослідження є з’ясувати поняття Smart School в концепції інфраструктури smart city. Наприклад концепцією проекту Kyiv Smart City [3] визначає пріоритетні рішення для розвитку міста: безпека, прозорість влади, розумний транспорт та електронні системи (рис. 1).

Впровадження мереж Wi-Fi. Smart City мають бути мобільними. Тому першим кроком є запровадження безкоштовної мережі Wi-Fi. Інтернет повинен покривати громадські місця, включаючи на подвір’ї школи, метро, автостоянки, двори та парки.

Системи відеоспостереження за прилеглою територією та в приміщеннях школи. Пропонується підвищити безпеку в місті шляхом запровадження систем відеоспостереження. Камери будуть встановлені в метро, на вулицях, перехрестях, у під'їздах житлових будинків та дворах, парках і місцях масового скупчення людей. Відеоінформація зберігатиметься на окремому сервері та за потреби передаватиметься правоохоронним органам.

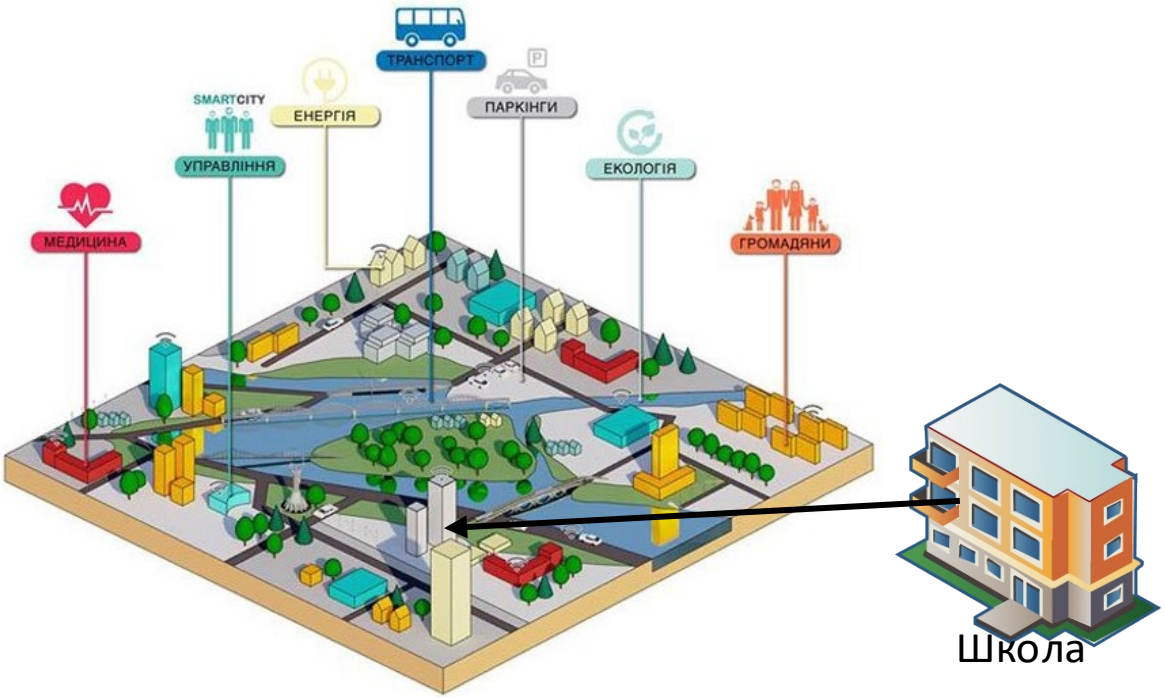


Рис. 1. Smart School в концепції інфраструктури Smart City

Розумне паркування біля школи. Статистика показує, що понад 30% заторів на дорогах спричинені тим, що водії шукають місця для паркування біля школи. Завдяки «розумному паркуванню» водії зможуть відстежувати завантаженість парковки навколо обораної школи і швидко дізнаватися, чи є вільні місця.

Камери зчитуватимуть номерні знаки припаркованих транспортних засобів, а система виписуватиме штраф, якщо оплата не буде здійснена більше необхідного часу для висадки/посадки дитини.

Розумне освітлення пришкільній території та у приміщеннях. Звичайні лампи замінять на світлодіодні та встановлять систему управління освітленням. Це значно зменшить витрати міста на вуличне освітлення та електроенергію. Наразі на освітлення витрачається від 18 до 30% міського бюджету.

Кнопки екстреного реагування. Встановлення кнопок екстреного реагування дозволить швидше передавати інформацію про правопорушення, що можуть виникнути в школах.

Smart School – система автоматизації для закладів загальної середньої освіти, професійно-технічних навчальних закладів та ВНЗ I - II рівнів акредитації. Таким чином розумна школа – це набір спеціалізованих інформаційних та цифрових технологій, які покращують комфортність навчання школярів, роботу та обслуговуючого персоналу.

Smart School має запропонувати всім учасникам освітнього процесу освітню цифрову платформу, яка максимально розкриє їхній освітній потенціал. Вони прямуватимуть шляхом, на якому будуть критично мислити та з легкістю долати усі виклики стандартів освіти сьогодення, підвищувати якість освітнього процесу.

До позитивних аспектів застосування Smart-технологій в навчальному процесі

школи відноситься наступне:

можливість їх використання під час викладання дисциплін природничо-математичного циклу;

підвищення інтересу учнів до навчання;

сучасність технологій, розуміння та сприймання їх учнями як природної складової молодих людей, що робить їх життя зручним інструментом для розвитку творчого потенціалу;

помірна легкість поєднання Smart-технологій з комунікативним підходом до викладання дисциплін природничо-математичного циклу;

зміну професійної діяльності з фізичної площини у віртуальний простір [4].

В умовах війни у Smart School простіше реалізувати безперервність освітнього процесу в умовах вимушеної перерви внаслідок повітряних тривог [5].

Отже, розвиток цифрових технологій настільки стрімкий, що вчені ще не зрозуміли можливості та межі їх застосування і розробили концепцію розумних міст як гуманітарного проекту для інклюзивного та безпечного розвитку людства. Впровадження smart-рішень у політику сучасних міст та шкіл є важливим соціальним і політичним проектом. Smart School можуть відповісти на виклики, пов'язані зі зростанням щільності населення та його постійним впливом на житлову і транспортну інфраструктуру. У міру того, як економіка стає все більш цифровою, з'являтиметься все більше і більше елементів розумних міст. Для того, щоб Smart School досягла всіх своїх цілей, ІКТ повинні активно розвиватися, не будучи «відрізаними» від інших елементів розвитку міської інфраструктури [6, с.63].

Література

[1] Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації» від 17.01.2018 №67-р. https://zakon.rada.gov.ua/laws/show/67-2018-p.

[2] Кайдан Т. Що таке smart city: в світі та в Києві. https://hmarochos.kiev.ua/2015/07/22/shho-take-smart-city-v-sviti-ta-v-kiyevi/.

[3] Про затвердження Концепції «Київ смарт сіті 2020. https://kyivcity.gov.ua/npa/pro_zatverdzhennya_kontseptsi_kiv_smart_siti_2020_348234/File_4xv2dcmgex_500-3507.pdf.

[4] Козубцов І.М. Модель системи ступеневої підготовки майбутніх науково-педагогічних працівників закладів вищої освіти до наукової діяльності в «цифровому освітньо-науковому середовищі». *Вісник науки та освіти. (Серія «Педагогіка»)*. 2023. №6(12). С. 414 – 430.

[5] Козубцов І.М. Методика викладання окремих навчальних дисциплін здобувачам вищої освіти в умовах воєнного часу. *Розвиток педагогічної науки і практики в умовах воєнного та повоєнного часу*: матеріали Звітної науково-практичної конференції Інституту педагогічної освіти і освіти дорослих імені Івана Зязюна НАПН України за 2022 рік (Київ, 16-23 березня 2023 р.). Київ: Інститут педагогічної освіти і освіти дорослих імені Івана Зязюна НАПН України, 2023. С. 125 – 128.

[6] Маркевич К. SMART-інфраструктура у сталому розвитку міст: світовий досвід та перспективи України. Київ: Видавництво “Заповіт”, 2021. 400 с.

АВТОНОМНИЙ НАВІГАЦІЙНИЙ ПРИСТІЙ ІНЕРЦІАЛЬНОГО ТИПУ

Вадим ЛУЦЕНКО (к.т.н., доцент)[1]
Олександр ГАВРЮКОВ (д.т.н., професор)[2]
Ольга БОНДАРЧУК (к.т.н., доцент)[3]

Київський національний університет будівництва та архітектури, факультет автоматизації і інформаційних технологій, кафедра автоматизації технологічних процесів, Київ, Україна
[1] lutsenko.viu@knuba.edu.ua, [2] havriukov.ov@knuba.edu.ua, [3] bondarchuk.ov@knuba.edu.ua

Abstract
The analysis was carried out and a list of the main requirements and functions of an autonomous navigation device of the inertial type was formed. The structure of the data logger was proposed. Work modes were determined and the work algorithm was created. The software is developed and the circuit board is built.

Вступ

Навігаційні системи інерційного типу – це системи, що використовуються для визначення положення, швидкості та орієнтації об'єкта в просторі без використання сигналів супутникових навігаційних систем або наземних маяків.

Ці системи мають широку область застосування в авіаційній промисловості для управління польотом та навігації літаків, космічних апаратів, у морській навігація для визначення положення кораблів та підводних човнів, в складі автономних транспортних засобів для вирішення задач самонаведення та керування. Такий широкий спектр напрямків застосування обумовлений можливістю автономної роботи, високою точністю позиціонування та орієнтації на невеликих відстанях, високою швидкістю реакції на зміни положення об'єкта.[1]

У той же час системам інерційної навігації притаманне накопичення помилок при тривалому використанні, чутливість до вібрацій, температурних змін та інших зовнішніх факторів. Створення і вдосконалення навігаційних систем інерційного типу потребує додаткових досліджень, розробки якісно нових моделей та підходів до проектування, що в свою чергу передбачає розробку та використання блоків для вимірювання та фіксації сигналів навігаційних датчиків. Такий пристрій називається даталоггером, а його розробка здійснена в ході проведеного дослідження.

Ефективне застосування даталоггера передбачає виконання та забезпечення ряду вимог і функцій, основними серед яких є:

1. Інформація від інерційних датчиків повинна зберігатися на зовнішньому носії даних (наприклад, SD-карті).
2. Забезпечити високу швидкість збору даних.

3. Забезпечити підтримку достатньої ємності пам'яті, що дозволить зберігати інформацію за тривалі періоди часу роботи.
4. Забезпечити синхронізацію даних із зовнішніми джерелами часу або геопозиціонування, що підвищить точність та зручність подальшого аналізу даних.
5. Компактний розмір та надійність.
6. Мати необхідні інтерфейси для вивантаження даних на комп'ютер або інші пристрої для подальшого аналізу, обробки та візуалізації.
7. Забезпечити стійкість та захищеність від вібрацій, екстремальних температур та інших впливів.

Вибір елементної бази проекту проводився з урахуванням зазначених функціональних вимог, доповнених критерієм мінімальної вартості.

У якості мікроконтролера використано 32-х розрядний ARM мікроконтролер Nuvoton M051, що відноситься до сімейства Cortex M0.

До складу мінімального набору навігаційних датчиків ввійшли:

- LSM 9DS0 – 3-х осьовий акселерометр та магнітометр;
- L3GD20H – 3-х осьовий гіроскоп;
- BMP 180 – датчик абсолютного атмосферного тиску.[2]

Для отримання міток часу, що відповідатимуть проведеним вимірюванням до складу даталоггера включено годинник реального часу на мікросхемі DS3231.

Людино-машинного інтерфейс користувача було організовано на базі мініатюрного OLED дисплея розміром 128x68 на базі драйвера SSD 1306 та електромеханічного енкодера PEC-11R.

Для збереження отриманої вимірювальної інформації використано flash карту пам’яті формату microSD ємністю 16Гб.

Усі периферійні пристрої, за виключенням карти пам’яті, підключені до мікроконтролера по шині I2C, що працює на частоті 400Гц. Flash накопичувач підключено по шині SPI. Структурна схема даталоггера наведена на рис.1.

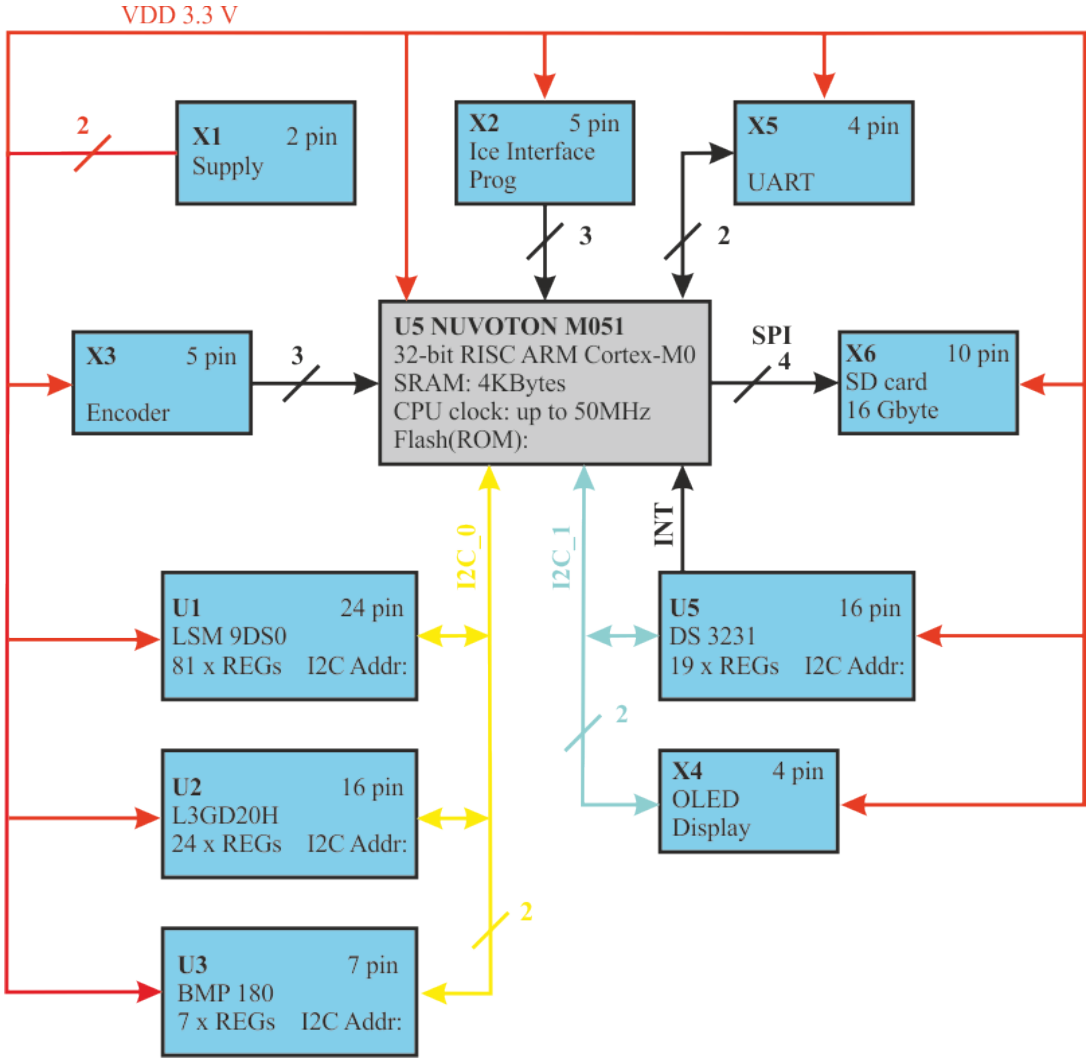


Рис.1. Структурна схема автономного навігаційного пристрою інерціального типу.

Алгоритм вимірювань передбачає, що вимірювання виконуються серіями. Кожна серія розпочинається за сигналом від годинника реального часу, частота якого складає 1Гц. Спочатку дані зчитуються з мікросхеми LSM 9DS0 потім L3GD20H та BMP 180. У кінці кожного зчитування ініціалізується процес запису отриманих даних на карту пам'яті. Після чого процес вимірювання буде повторюватись аж до появи чергового сигналу від годинника реального часу. Кожна серія вимірювань містить близько 1000 результатів для кожного параметру.

Дані, що записуються на карту пам'яті доповнюються мітками часу, які формуються з використанням поточного часу, що отримується від мікросхеми DS3231.

Алгоритм роботи даталоггера передбачає декілька режимів роботи.

1. Режим автономного функціонування з фіксацією отриманих даних. У цьому режимі відбуваються вимірювання та запис їх результатів на карту пам'яті. Вивід даних на дисплей не передбачається.

2. Режим автономного функціонування з фіксацією даних, що перевищують задане порогове значення. Порогові значення задаються по кожному параметру окремо. Вивід даних на дисплей не передбачається.
3. Сервісний режим_1 передбачає проведення вимірювань з відображенням отриманих результатів на дисплеї без їх запису на карту пам'яті.
4. Сервісний режим_2 дозволяє провести налаштування порогів спрацювання, встановити значення поточної дати та часу, обрати режим роботи.

Програмне забезпечення даталоггера розроблено на мові С з використанням процедурного підходу. Створено окремі функції, що реалізують опитування датчиків, навігацію по меню, відображення вимірювальної інформації в реальному часі. Окрему частину програмного забезпечення складають три службових модулі: модуль, що реалізує інформаційний обмін по шині I2C; модуль, що забезпечує вивід даних на OLED дисплей; та модуль читання-запису даних на карту пам'яті. Відзначимо, що розробка програмного забезпечення проводилась в середовищі Keil uVision 4 з використанням прототипів функцій для роботи з периферійними пристроями мікроконтролера, які утворюють – Board Support Package (BSP).[3] Такий підхід забезпечує певний рівень абстракції на апаратному рівні і, безумовно, сприяє підвищенню швидкості розробки.

З використанням САПР Altium розроблено комплект конструкторської документації для виготовлення двошарової друкованої плати даталоггера. З метою забезпечення зручності монтажу та необхідністю підвищення вібростійкості шляхом заповнення простору між елементами вологостійким компаундом, мікроконтролер, часи реального часу та датчики розміщені на верхній поверхні плати, в той час як карман карти пам'яті знаходиться на нижній. Також на платі розміщено окремі роз'єми для підключення живлення, дисплея та енкодера. Розроблений пристрій має автономне акумуляторне живлення з можливістю індикації на дисплеї рівня заряду. На рис.2 представлено 3D модель розробленого пристрою.

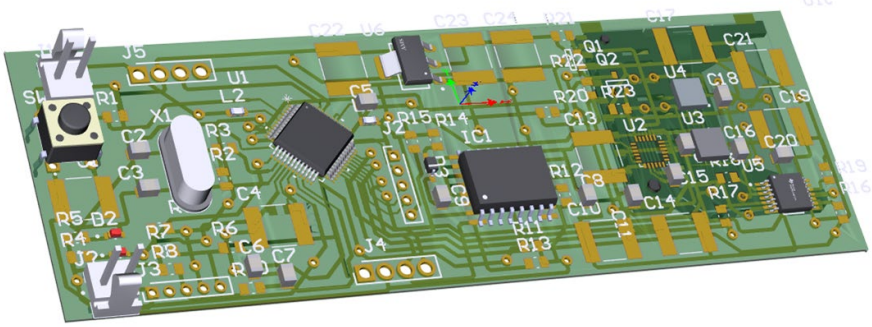


Рис.2. 3D модель даталоггера

Навігаційні системи інерційного типу є важливим елементом систем управляння транспортом, що забезпечує автономне позиціонування та орієнтацію об'єктів у просторі. Розробка та вдосконалення таких систем потребує отримання

інформації про параметри руху. Забезпечити в реальному часі такий моніторинг кутової швидкості, лінійного прискорення, магнітного поля та атмосферного тиску вдається за допомогою спеціальних пристроїв – даталоггерів, що містять відповідні датчики. Слід відзначити, що практичне використання розробленого даталоггеру потребує додаткових досліджень, метою яких є визначення його реальних метрологічних характеристик.

Література

[1] Michael Braasch. Fundamentals of Inertial Navigation Systems and Aiding. – Ohio University Avionics Engineering Center (AEC), USA.–2022.– 412P.
[2] MEMS and Sensors [Електронний ресурс] // URL: https://www.st.com/en/mems-and-sensors.html.
[3] The Board Support Package(BSP) CMSIS for M051 series. [Електронний ресурс] // URL: https://www.nuvoton.com/products/microcontrollers/arm-cortex-m0-mcus/m051-base-series/m0515lde/?tab=2&group=Software&rt=Board%20Support%20Package%20(BSP).

МЕТОДИ І ІНСТРУМЕНТИ СТАТИЧНОГО АНАЛІЗУ, МОДУЛЬНОГО ТА ІНТЕГРАЦІЙНОГО ТЕСТУВАННЯ У ВБУДОВАНИХ СИСТЕМАХ

Олексій ПАВЛЮК (студент)

Київський національний університет будівництва і архітектури, факультет автоматизації і інформаційних технологій, кафедра кібербезпеки та комп'ютерної інженерії, Київ, Україна
alexpavluk10@gmail.com

Анотація
Мета цієї роботи охарактеризувати основні методи і інструменти, які використовуються у вбудованих системах для проведення статичного аналізу, модульного тестування та інтеграційного тестування. Також розглянуто як ці методи та інструменти інтегруються в концепції V-моделі та керованій тестами розробці.

Abstract
The purpose of this paper is to describe the main methods and tools used in embedded systems for static analysis, unit testing, and integration testing. It also describes how these methods and tools are integrated into the concepts of the V-model and Test-Driven Development.

Вступ

Вбудовані системи (з англ. «embedded systems») є необхідною складовою багатьох пристроїв, від побутових електронних пристроїв до автомобілів та медичних пристроїв, які взаємодіють в концепції Інтернету речей. У зв'язку зі стрімким зростанням індустрії вбудованих систем, якість коду вбудованих пристроїв стала однією з головних проблем. Враховуючи специфіку розробки вбудованих систем (складність налагодження, висока ціна помилки тощо), розробникам необхідно використовувати спеціальні інструменти для підвищення якості коду.

Методи і інструменти для статичного аналізу у вбудованих системах

Статичний аналіз - це метод, що дозволяє аналізувати програмний код без його виконання з метою виявлення помилок, аномалій та можливих проблем. Інструменти статичного аналізу виконують глибшу перевірку вихідного коду, ніж компілятори. Зазвичай компілятори знаходять лише синтаксичні помилки.

Статичні аналізатори можуть виконувати широкий спектр завдань. Деякі з найпопулярніших такі [1]:

1. виявлення помилок у програмному коді. У цьому випадку статичний аналіз значно доповнює огляд коду.

2. підвищення якості коду в широкому сенсі. Якість коду може включати читабельність, оптимізацію, складність коду, рівень зв'язності та інші аспекти.
3. аналіз коду як частина механізму Quality Gates (вид контролю за якістю, в якому процес перевірки представлений у вигляді набору «воріт» із списком завдань/вимог) в CI/CD (Continuous Integration/Continuous Delivery).
4. вони зупиняють безперервну розробку коду, якщо рівень якості не відповідає заданим вимогам.

Методи і інструменти для модульного тестування у вбудованих системах

Модульне тестування (з англ. «unit testing») означає ізольоване тестування невеликих частин програмного забезпечення від більшої системи за допомогою автоматизованих тестів. Це дозволяє тестувати їх окремо від інших частин системи, які можуть бути ще не готові. Зокрема, для вбудованих систем це означає тестування не на цільовому обладнанні, а на хості розробки або сервері збірки. Сучасною версією модульного тестування є керована тестами розробка (з англ. «Test-Driven Development») [2].

В якості інструментів можуть використовуватися такі системи:

1. Фреймворки. Це програмні бібліотеки та інструменти, які допомагають розробникам створювати та виконувати модульні тестування. Прикладами є Google Test, Unity, Ceedling тощо.
2. Засоби автоматизації тестування. Вони допомагають автоматизувати процес створення, виконання та аналізу. Наприклад, Jenkins, Azure DevOps, TeamCity тощо.

Методи і інструменти для інтеграційного тестування у вбудованих системах

Інтеграційне тестування (з англ. «integration testing») – це процес тестування взаємодії між компонентами системи, щоб переконатися, що вони працюють разом правильно. Інтеграційне тестування вбудованих систем передбачає об'єднання блоків у модулі та тестування цих модулів або груп модулів. Метою інтеграційного тестування є виявлення недоліків, оскільки модулі тестуються в поєднанні.

Окремих методів для інтеграційного тестування немає. Для кожного окремого випадку системи можуть тестуватися різні набори компонентів системи [3].

Застосування методів і інструментів тестування у V-моделі

V-модель – це методологія розробки вбудованих систем, де робочий процес розбивається на етапи, і для кожного етапу виконується певна послідовність тестування. У V-моделі тестування виконується на різних етапах:

1. Статичний аналіз використовується на початкових етапах розробки для виявлення та виправлення помилок перед переходом до наступних етапів. Це перший етап тестування в моделі.
2. Модульне тестування проводиться на етапі розробки окремих компонентів. Кожен компонент тестується індивідуально для переконання в його правильному функціонуванні.
3. Інтеграційне тестування включає в себе тестування взаємодії між компонентами. Застосовується перед останнім системним тестуванням.

Застосування методів і інструментів тестування у КТР

Керована тестами розробка (КТР) – це методологія розробки, де програмісти спочатку створюють тести для функціоналу, який ще не існує, а потім розробляють код, який пройшов би ці тести.

Робочий процес КТР відбувається за простим циклом:

1. Напишіть невеликий тест для перевірки поведінки.
2. Створіть і запустіть набір тестів, щоб побачити, що новий тест не пройшов, можливо, навіть не скомпілювався.
3. Внесіть зміни до коду, необхідні для проходження тесту.
4. Зберіть і запустіть набір тестів, щоб побачити, що новий тест пройшов.
5. Проведіть рефакторинг, щоб видалити дублювання або почистити тест.

Для того, щоб цей цикл був швидким (від кількох секунд до кількох хвилин), кожна ітерація повинна містити мінімально можливу кількість коду. Коли тест несподівано не проходить (або проходить, коли очікувалось, що він не пройде), ви чітко знаєте, що проблема обмежена цією невеликою кількістю коду.

Статичний аналіз може бути використаний для перевірки якості нового коду та виявлення помилок на ранніх етапах.

Модульне тестування і є КТР, оскільки це його попередник.

Інтеграційне тестування може бути використане для тестування взаємодії нового функціоналу з іншими компонентами системи.

Висновки

У вбудованих системах важливо застосовувати методи і інструменти статичного аналізу, модульного тестування та інтеграційного тестування для забезпечення якості та надійності. Їх застосування у V-моделі та КТР дозволяє виявляти та виправляти помилки на всіх етапах розробки, зменшуючи ризики та витрати.

Правильне поєднання цих методів і інструментів допомагає створити високоякісні вбудовані системи, які відповідають вимогам та очікуванням замовників і користувачів.

Література

[1] Static Analysis in Embedded System Development by Maxim Stefanov 202: https://embeddedcomputing.com/technology/debug-and-test/code-analysis-tools/static-analysis-in-embedded-system-development.
[2] Unit Testing For Embedded Software Development by Steve Branam 2022: https://dojofive.com/blog/unit-testing-for-embedded-software-development/.
[3] Quality Gates in Testing - Powerful but underused! by Gipil Quddus 2020: https://www.linkedin.com/pulse/quality-gates-testing-powerful-underused-gipil-quddus/.
[4] What is Test Driven Development (TDD)? by Jash Unadkat, 2023: https://www.browserstack.com/guide/what-is-test-driven-development.

ІНТЕРНЕТ РЕЧІ ТА РОЗУМНИЙ ДІМ

Дмитро ДУДИНЕЦЬ (студент)

Київський національний університет будівництва і архітектури, факультет автоматизації і інформаційних технологій, кафедра кібербезпеки та комп'ютерної інженерії, Київ, Україна

Анотація

Системи розумного будинку набули великої популярності в останні десятиліття, оскільки вони підвищують комфорт і якість життя. Більшість систем розумного будинку контролюються смартфонами та мікроконтролерами. Додаток для смартфона використовується для контролю та моніторингу домашніх функцій за допомогою бездротових методів зв'язку. Концепція розумного будинку з інтеграцією в нього сервісів IoT і хмарних обчислень, шляхом вбудовування інтелекту в датчики і виконавчі механізми, об'єднання розумних речей в мережу з використанням відповідної технології, полегшення взаємодії з розумними речами за допомогою хмарних обчислень для легкого доступу в різних місцях, збільшення обчислювальної потужності, простору для зберігання даних і підвищення ефективності обміну даними. У цій главі ми представляємо композицію з трьох компонентів для побудови надійного підходу до концепції та реалізації передового розумного будинку.

Ключові слова

Розумний дім, IoT, хмарні обчислення, обробка подій, побутова техніка, обробка подій на основі правил.

Вступ

Класичний розумний будинок, інтернет речей, хмарні обчислення і обробка подій на основі правил - це будівельні блоки запропонованої мною комплексної системи розумного будинку. Кожен компонент вносить свої основні атрибути і технології в запропоновану композицію. IoT забезпечує підключення до інтернету та дистанційне керування мобільними пристроями, поєднаними з різноманітними датчиками. Датчики можуть бути прикріплені до побутових приладів, таких як кондиціонери, освітлення та інші екологічні пристрої. Таким чином, хмарні обчислення вбудовують комп'ютерний інтелект у домашні пристрої, щоб забезпечити способи вимірювання домашніх умов і моніторингу функціональності побутової техніки. Хмарні обчислення надають масштабовану обчислювальну потужність, простір для зберігання даних і додатки для розробки, обслуговування, запуску домашніх сервісів і доступу до домашніх пристроїв з будь-якого місця і в будь-який час. Система обробки подій на основі правил забезпечує контроль і оркестровку всієї складної системи "розумного будинку".

1. Класичний огляд розумного будинку

Розумний дім - це житлове розширення автоматизації будівлі, що включає в себе контроль і автоматизацію всіх вбудованих технологій. Він визначає житло, в якому є побутова техніка, освітлення, опалення, кондиціонери, телевізори, комп'ютери, розважальні системи, велика побутова техніка, така як пральні/сушильні машини і холодильники/морозильники, системи безпеки і відеоспостереження, здатні взаємодіяти один з одним і управлятися дистанційно за розкладом, телефоном, мобільним зв'язком або через мережу Інтернет. Ці системи складаються з перемикачів і датчиків, підключених до центрального вузла, яким керує мешканець будинку за допомогою настінного терміналу або мобільного пристрою, підключеного до хмарних інтернет-сервісів.

Розумний будинок забезпечує безпеку, енергоефективність, низькі експлуатаційні витрати та зручність. Встановлення розумних продуктів забезпечує зручність та економію часу, грошей та енергії. Такі системи є адаптивними і налаштовуються відповідно до постійних мінливих потреб мешканців будинку. У більшості випадків їхня інфраструктура достатньо гнучка, щоб інтегруватися з широким спектром пристроїв різних постачальників і стандартів.

Популярність і проникнення концепції розумного будинку зростає хорошими темпами, оскільки вона стала частиною тенденцій модернізації та скорочення витрат. Це досягається завдяки можливості ведення централізованого журналу подій, виконання процесів машинного навчання для забезпечення основних елементів витрат, рекомендацій щодо економії та інших корисних звітів.

1.1 Послуги розумного будинку

1.1.1 Вимірювання домашніх умов

Типовий розумний будинок оснащений набором датчиків для вимірювання домашніх умов, таких як: температура, вологість, освітленість і близькість. Кожен датчик призначений для вимірювання одного або декількох параметрів. Температура і вологість можуть вимірюватися одним датчиком, інші датчики обчислюють коефіцієнт освітленості для даної зони і відстань від неї до кожного об'єкта, що потрапляє в неї. Всі датчики дозволяють зберігати дані та візуалізувати їх, щоб користувач міг переглянути їх будь-де і будь-коли. Для цього він включає в себе процесор сигналу, інтерфейс зв'язку та хост на хмарній інфраструктурі.

1.1.2 Керування домашньою технікою

Створюється хмарний сервіс для керування домашніми приладами, який буде розміщено на хмарній інфраструктурі. Сервіс дозволяє користувачеві керувати виходами інтелектуальних приводів, пов'язаних з домашніми приладами, такими

як лампи та вентилятори. Розумні приводи - це пристрої, такі як клапани і перемикачі, які виконують такі дії, як вмикання або вимикання або налаштування операційної системи. Приводи забезпечують різноманітні функціональні можливості, такі як увімкнення/вимкнення клапана, позиціонування на відсоток відкриття, модуляція для управління змінами умов потоку, аварійне вимкнення (ESD). Щоб активувати привід, на нього подається команда цифрового запису.

1.1.3 Керування домашнім доступом

Технології домашнього доступу зазвичай використовуються для дверей громадського доступу. Звичайна система використовує базу даних з ідентифікаційними атрибутами уповноважених осіб. Коли людина наближається до системи контролю доступу, її ідентифікаційні атрибути миттєво зчитуються і порівнюються з базою даних. Якщо вони збігаються з даними бази даних, доступ дозволяється, в іншому випадку - відмовляється. Для широко розподіленої установи можна використовувати хмарні сервіси для централізованого збору даних осіб та їх обробки. Чи використовувати магнітні або безконтактні ідентифікаційні картки, інші - системи розпізнавання обличь, відбитків пальців і RFID.

1.2 Основні компоненти

Для виконання всіх вищеописаних дій та управління даними система складається з наступних компонентів, як показано на рисунку 1.

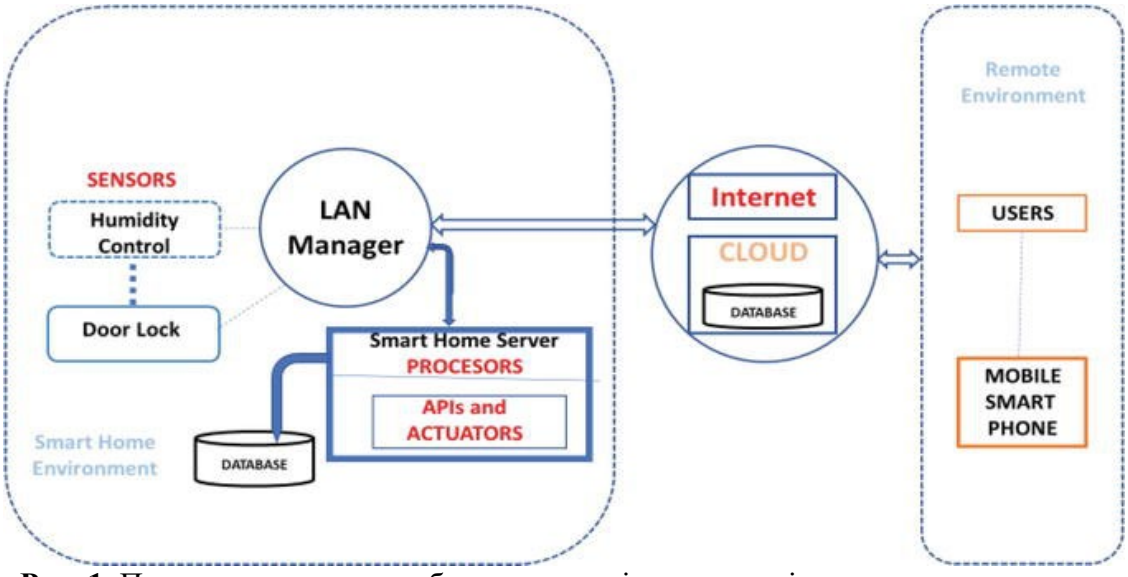


Рис. 1. Парадигма розумного будинку з опціональним підключенням до хмари.

Датчики для збору внутрішніх і зовнішніх даних про будинок та вимірювання умов у ньому. Ці датчики під'єднані до самого будинку і до підключених до нього пристроїв. Ці датчики не є датчиками інтернету речей, які під'єднуються до

побутової техніки. Дані датчиків збираються і безперервно передаються через локальну мережу на сервер розумного будинку. Процесори для виконання локальних та інтегрованих дій. Він також може бути підключений до хмари для додатків, що вимагають розширених ресурсів. Дані з датчиків обробляються процесорами локального сервера.

Набір програмних компонентів, загорнутих у вигляді API, що дозволяє зовнішнім додаткам виконувати його, якщо вони дотримуються попередньо визначеного формату параметрів. Такий API може обробляти дані з датчиків або керувати необхідними діями.

Актуатори для надання та виконання команд на сервері або інших пристроях керування. Перекладає необхідну дію в синтаксис команди, яку пристрій може виконати. Під час обробки отриманих даних з датчиків задача перевіряє, чи спрацювало якесь правило. У такому випадку система може запустити команду відповідному процесору пристрою.

База даних для зберігання оброблених даних, зібраних з датчиків [та хмарних сервісів]. Вона також буде використовуватися для аналізу, представлення та візуалізації даних. Оброблені дані зберігаються в доданій базі даних для подальшого використання.

2. Огляд IoT

Парадигма (IoT) відноситься до пристроїв, підключених до інтернету. Пристрої - це такі об'єкти, як датчики і виконавчі механізми, оснащені телекомунікаційним інтерфейсом, процесором, обмеженим обсягом пам'яті і програмним забезпеченням. Це дозволяє інтегрувати об'єкти в інтернет, встановлюючи взаємодію між людьми та пристроями між пристроями. Ключовими технологіями IoT є радіочастотна ідентифікація (RFID), сенсорні технології та інтелектуальні технології. RFID є основою і мережевим ядром побудови IoT. Її можливості обробки і зв'язку разом з унікальними алгоритмами дозволяють об'єднувати різні елементи в єдине ціле, але в той же час дозволяють легко додавати і видаляти компоненти з мінімальним впливом, роблячи IoT надійним, але гнучким, щоб адаптуватися до змін в навколишньому середовищі і вподобань користувачів. Для мінімізації використання пропускної здатності використовується JSON, полегшена версія XML, для обміну повідомленнями між компонентами та зовнішніми повідомленнями.

3. Хмарні обчислення та їхній внесок в IoT і розумний дім

Хмарні обчислення - це спільний пул обчислювальних ресурсів, готовий до надання різноманітних обчислювальних послуг на різних рівнях, від базової інфраструктури до найскладніших прикладних сервісів, які легко розподіляються

і вивільняються з мінімальними зусиллями або взаємодією з постачальниками послуг. На практиці хмара управляє обчислювальними, сховищними та комунікаційними ресурсами, які спільно використовуються багатьма користувачами у віртуалізованому та ізольованому середовищі. На рисунку 2 зображено загальну парадигму хмарних технологій.

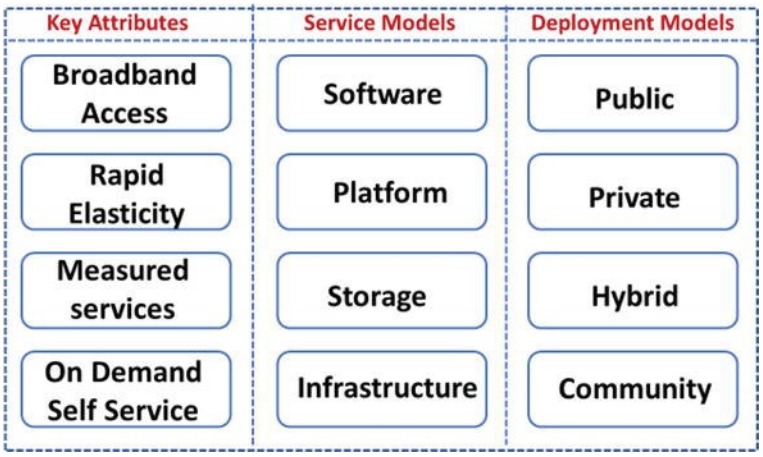


Рис. 2. Парадигма хмарних обчислень.

IoT та "розумний дім" можуть скористатися широкими ресурсами та функціоналом хмарних обчислень, щоб компенсувати їхні обмеження у зберіганні, обробці, комунікації, підтримці попиту, резервному копіюванні та відновленні. Наприклад, хмара може підтримувати управління послугами Інтернету речей і виконувати додаткові додатки, використовуючи дані, отримані з неї. Розумний дім може бути стислим і зосередитися лише на основних і критично важливих функціях, а отже, мінімізувати локальні домашні ресурси і покладатися на можливості і ресурси хмари. Розумний дім та Інтернет речей зосереджуватимуться на зборі даних, їх базовій обробці та передачі в хмару для подальшої обробки. Щоб впоратися з проблемами безпеки, хмара може бути приватною для високозахищених даних і загальнодоступною для решти.

IoT, розумний дім і хмарні обчислення - це не просто злиття технологій. Це радше баланс між локальними та центральними обчисленнями, а також оптимізація споживання ресурсів. Обчислювальну задачу можна виконати на пристроях Інтернету речей і розумного будинку або віддати на аутсорсинг у хмару. Вибір місця для обчислень залежить від компромісу між накладними витратами, доступністю даних, залежністю від даних, обсягом транспортування даних, залежністю від зв'язку та міркувань безпеки. З одного боку, потрійна модель обчислень, що включає хмару, Інтернет речей і розумний будинок, повинна мінімізувати вартість всієї системи, зазвичай з більшим акцентом на скорочення споживання ресурсів вдома. З іншого боку, модель обчислювальних послуг IoT і "розумного будинку" повинна поліпшити роботу користувачів IoT, щоб задовольнити їхні потреби при використанні хмарних додатків і вирішити складні

проблеми, що виникають у зв'язку з новою моделлю послуг IoT, "розумного будинку" і хмарних сервісів.

4. Централізована обробка подій, система на основі правил

Розумний дім та IoT насичені датчиками, які генерують величезні потоки даних у вигляді повідомлень або подій. Обробка цих даних перевищує можливості людини. Тому для швидшого реагування на класифіковані події були розроблені та використовуються системи обробки подій. Користувач може визначити правило, що спрацьовує за певною подією, і контролювати належне надання послуг. Правило складається з умов події, шаблону події та кореляційної інформації, які можна комбінувати для моделювання складних ситуацій.

Система може обробляти велику кількість подій, виконувати функції моніторингу, навігації та оптимізації процесів у режимі реального часу. Вона виявляє та аналізує аномалії або винятки і створює реактивні/проактивні реакції, такі як попередження та дії, що запобігають пошкодженню. Ситуації моделюються за допомогою зручного інтерфейсу моделювання для правил, що запускаються подіями. За необхідності він розбиває їх на прості, зрозумілі елементи. Запропонована модель може бути легко інтегрована в розподілену і сервіс-орієнтовану платформу обробки подій.

Процес оцінювання запускається подіями, які надають найсвіжішу інформацію про стан та інформацію з відповідного середовища. Результатом є граф рішень, що представляє правило. Він може розбивати складні ситуації на прості умови, а також комбінувати їх один з одним, створюючи складні умови. Результатом є подія реагування, що виникає, коли правило спрацьовує. Спрацьовані події можуть бути використані як вхідні дані для інших правил для подальшої оцінки. Шаблони подій виявляються, коли відбувається кілька подій, які відповідають заздалегідь визначеному шаблону. Завдяки графічній моделі та модульному підходу до побудови правил, правила можуть бути легко адаптовані до змін домену. Нові умови подій або шаблони подій можуть бути додані або видалені з моделі правил. Правила виконуються за допомогою сервісів подій, які постачають рушій правил подіями і обробляють результат оцінки. Для забезпечення доступності відповідних обчислювальних ресурсів система може працювати в розподіленому режимі, на декількох машинах, а також полегшує інтеграцію із зовнішніми системами. Визначення зв'язків і залежностей між подіями, які є релевантними для обробки правил, здійснюється за допомогою наборів послідовностей, що генеруються механізмом правил. Механізм правил будує послідовності подій, релевантні певній умові правила, що дозволяє асоціювати події за їхніми контекстними даними. Правила автоматично виконують дії у відповідь, коли вказані умови виконуються. Дії генерують події реагування, які запускають заходи реагування. Шаблони подій можуть відповідати часовим послідовностям

подій, що дозволяє описувати домашні ситуації, в яких настання подій є релевантним. Наприклад, коли двері залишаються відчиненими занадто довго.

За допомогою цієї моделі вирішуються такі завдання: структура для оброблюваних подій і даних, конфігурація сервісів і адаптерів для етапів обробки, включаючи їх вхідні і вихідні параметри, інтерфейси до зовнішніх систем для збору даних і реагування шляхом виконання транзакцій, структура для оброблюваних подій і даних, перетворення даних, аналіз даних і збереження даних. Це дозволяє моделювати, які події повинні оброблятися сервісом правил і як події-відповіді повинні перенаправлятися до інших сервісів подій. Процес простий: дані збираються та отримуються від адаптерів, які пересилають події до сервісів подій, що їх споживають. Спочатку події збагачуються, щоб підготувати дані для обробки правил. Наприклад, події-відповіді надсилаються до сервісу для надсилання сповіщень колл-агенту або до сервісів, які передають сповіщення про затримку події та оновлення подій назад до системи керування подіями.

5. Практичні аспекти та міркування щодо впровадження IoT та розумного дому

Розумний дім складається з трьох компонентів: обладнання, програмного забезпечення та комунікаційних протоколів. Він має широкий спектр застосувань для цифрового споживача. Деякі з сфер домашньої автоматизації, що базуються на підключенні до Інтернету речей, такі як: управління освітленням, садівництво, охорона і безпека, якість повітря, моніторинг якості води, голосові асистенти, вимикачі, замки, лічильники енергії та води.

Розширені компоненти розумного будинку включають в себе: IoT-датчики, шлюзи, протоколи, мікропрограми, хмарні обчислення, бази даних, проміжне програмне забезпечення та шлюзи. Хмару Інтернету речей можна розділити на платформу як послугу (PaaS) та інфраструктуру як послугу (IaaS). На рисунку 4 показані основні компоненти пропонованого вдосконаленого розумного будинку, а також зв'язок і потік даних між його компонентами.

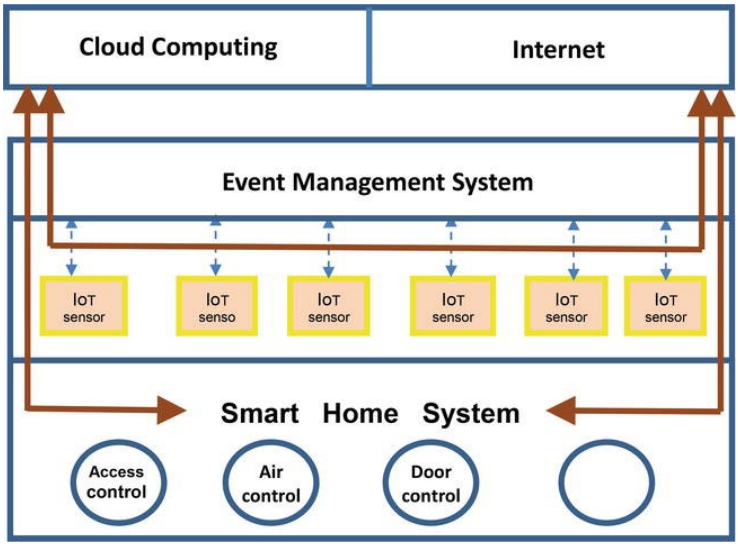


Рис. 4. Розширений склад розумного будинку.

Додаток розумного будинку оновлює базу даних будинку в хмарі, щоб дозволити віддаленим людям отримати доступ до неї і отримати останній стан будинку. Типова платформа IoT містить: безпеку і автентифікацію пристроїв, брокери повідомлень і черги повідомлень, адміністрування пристроїв, протоколи, збір даних, візуалізацію, можливості аналізу, інтеграцію з іншими веб-сервісами, масштабованість, API для потоку інформації в реальному часі і бібліотеки з відкритим вихідним кодом. Датчики Інтернету речей для домашньої автоматизації відомі своїми сенсорними можливостями, такими як: температура, освітленість, рівень води, склад повітря, відеокамери спостереження, голос/звук, тиск, вологість, акселерометри, інфрачервоні, вібраційні та ультразвукові датчики. Одними з найпоширеніших датчиків розумного будинку є датчики температури, більшість з яких є цифровими, але є й аналогові, які можуть бути надзвичайно точними. Датчики освітленості вимірюють яскравість. Ультразвукові датчики рівня води.

Протоколи зв'язку розумного будинку: Bluetooth, Wi-Fi або GSM. Bluetooth - це інтелектуальні або низькоенергетичні бездротові протоколи з можливостями комірчастої мережі та алгоритмами шифрування даних. Zigbee - комірчаста мережа, малопотужний радіочастотний протокол для IoT. X10 - протокол, який використовує проводку лінії електропередач для сигналізації та управління. Крім того, бездротовий та дротовий зв'язок. Z-wave спеціалізується на захищеній домашній автоматизації. UPB, використовує існуючі лінії електропередач. Thread, безоплатний протокол для автоматизації розумного будинку. ANT, протокол з наднизьким енергоспоживанням для побудови малопотужних датчиків з можливістю розподілу по сітці. Найбільш популярними протоколами є bluetooth low energy, Z-wave, Zigbee та thread. Міркування щодо включення шлюзу можуть включати: підключення до хмари, підтримувані протоколи, складність

кастомізації та підтримку прототипів. Внутрішнє управління складається з наступних компонентів: машина станів, шина подій, журнал обслуговування і таймер.

6. Приклади розумного дому та IoT

У літературі та практичних звітах можна знайти багато реалізацій різноманітних інтеграцій між трьома основними будівельними блоками - "розумним будинком", IoT та хмарними обчисленнями. У цьому розділі розглянемо три реалізації, які наочно демонструють необхідність і переваги взаємозв'язку або інтеграції всіх трьох компонентів, як показано на рисунку 5. Кожен компонент пронумеровано від 1 до 6. У лівій частині описує для кожної реалізації послідовність повідомлень/команд між компонентами, зліва направо і знизу вгору. Візьмемо для прикладу третю реалізацію: задача управління, яка постійно працює на домашньому сервері (2), виявляє той факт, що всі мешканці покинули будинок, і автоматично запускає виконавчі механізми для вимкнення всіх IoT-пристроїв (3), після чого надсилає повідомлення відповідним користувачам/мешканцям, інформуючи їх про ситуацію та застосовані дії (6).

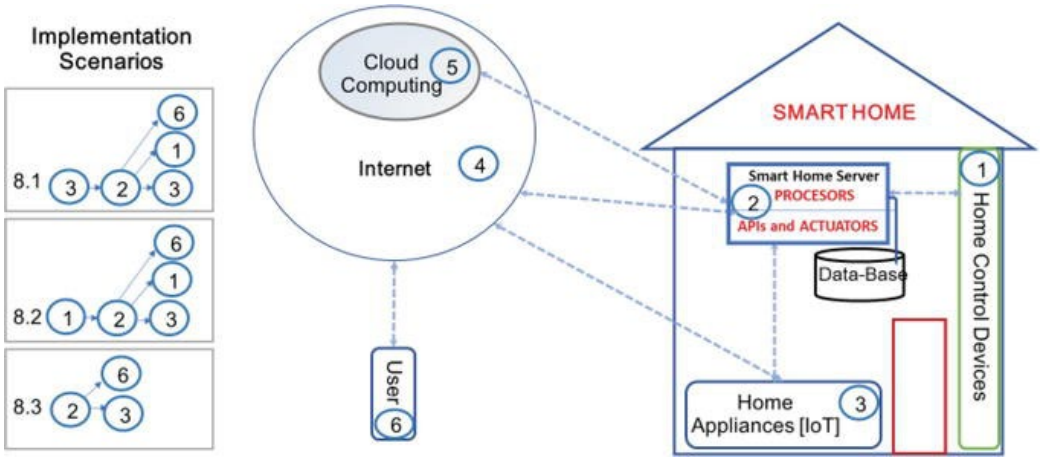


Рис 5. Діаграма реалізацій розширеного розумного будинку. Використання (і) в поясненні реалізацій відповідає обведеним цифрам на Рисунку 5.

6.1 Виявлення витоків води та їх запобігання

Першим кроком є встановлення датчиків води під кожним розумним потенційним джерелом витоку та автоматизованого головного датчика водяного клапана для всього будинку, що тепер означає, що будинок розглядається як IoT.

Якщо датчик води виявляє витік води (3), він надсилає подію на хаб (2), який запускає програму "перекрити кран". Потім програма для керування будинком надсилає команду "вимкнути" всім пристроям Інтернету речей (3), визначеним як чутливі до перекриття води, а потім надсилає команду "вимкнути" головному

водопровідному клапану (1). Повідомлення про оновлення надсилається через систему обміну повідомленнями на ці пристрої, що з'являються у списку сповіщень (6). Таке налаштування допомагає захиститися від сценаріїв, коли джерелом води є водопровідна система будинку. Базова конфігурація передбачає інтеграцію за допомогою повідомлень і команд між розумним будинком і системою управління IoT. Вона демонструє залежність і переваги поєднання розумного будинку та Інтернету речей.

6.2 Датчики диму

У більшості будинків вже є типовий набір датчиків диму (1), але немає моста для передачі даних з датчика на хаб розумного будинку. Підключення цих датчиків до застосунку розумного будинку (2) дає змогу створити комплексну систему виявлення диму. Її можна розширити, щоб сповіщати датчик ліфта про блокування його використання через пожежу (1), а потім ще більше розширити до будь-якого датчика Інтернету речей (3), який може бути активований через виявлений сигнал тривоги про задимлення.

6.3 Управління інцидентами для керування домашньою технікою

Розглянемо сценарій, коли деякі прилади залишаються ввімкненими. У разі тривалої відсутності деякі з них можуть перегрітися і перегоріти. Щоб уникнути таких ситуацій, підключаємо всі датчики IoT-приладів до домашнього застосунку (2), щоб коли всі підуть з дому, він автоматично налаштував датчики всіх приладів відповідним чином (3), щоб уникнути пошкоджень. Зверніть увагу, що індикація порожнього будинку генерується додатком "Розумний дім", тоді як індикація увімкненого приладу генерується IoT. Отже, цей сценарій можливий завдяки інтеграції між системами розумного дому та IoT.

Висновки

У цьому розділі я описав інтеграцію трьох слабо пов'язаних між собою компонентів: розумного будинку, IoT і хмарних обчислень. Для ефективного і збалансованого управління величезним потоком даних, використовуючи сильні сторони кожного компонента, я пропоную централізований додаток для обробки подій в реальному часі.

Я описую переваги та вигоди кожного окремого компонента та його можливі доповнення, які можуть бути досягнуті шляхом інтеграції з іншими компонентами, що забезпечить нові переваги, отримані від всієї системи в цілому. Оскільки ці компоненти все ще перебувають на стадії розробки, інтеграція між ними

може змінитися і забезпечити надійну парадигму, яка генерує нове покоління інфраструктури та додатків.

Література

[1] Stergioua C, Psannis KE, Kimb B-G, Gupta B. Безпечна інтеграція IoT та хмарних обчислень. Elsevier, Комп'ютерні системи майбутнього покоління, том 78. Частина 3. Січень 2018. с. 964-975.
[2] Аль-Куварі М., Рамадан А., Ісмаель Ю., Аль-Сугаїр Л., Гастлі А., Бенаммар М. Автоматизація розумного будинку з використанням платформи зондування та моніторингу на основі Інтернету речей, IEEE. 2018.
[3] Датта Т., Апторп Н., Феастер Н. Зручна для розробників бібліотека для обфускації трафіку розумного будинку IoT, що зберігає конфіденційність, IoT S&P 18. In: Матеріали семінару 2018 року з безпеки та конфіденційності IoT. ACM; 2018. стор. 43-48.
[4] Мао Дж, Лін К, Бьян Дж. Застосування алгоритмів навчання в системі безпеки IoT-систем розумного будинку. Американський інститут математичних наук; 2018. DOI: 10.3934/mfc.2018004.
[5] Saeed F, Paul A, Rehman A, Hong WH, Seo H. Інтелектуальне моделювання середовища розумного будинку на основі IoT для запобігання пожежі та безпеки. Журнал мереж датчиків та приводів. 2018;7(1):11. DOI: 10.3390/jsan7010011.
[6] Botta A, de Donato W, Persico V, Pescapé A. Інтеграція хмарних обчислень та інтернету речей: Опитування. Комп'ютерні системи майбутнього покоління. 2016; 56:684-700.
[7] Soliman M, Abiodun T, Hamouda T, Zhou J, Lung C-H. Розумний дім: Інтеграція інтернету речей з веб-сервісами та хмарними обчисленнями. В кн: Міжнародна конференція з технологій хмарних обчислень і науки; IEEE. 2013.
[8] Пашке А., Козленков А. Обробка подій на основі правил і правила реакції. Лондон: Betfair Ltd; 2009. DOI: 10.1007/978-3-642-04985-98.

ТЕХНОЛОГІЯ ХМАРНОГО СХОВИЩА В СФЕРІ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

Євген ЛАВОШНИК (студент)
Ярослав МАШЕВСЬКИЙ (студент)

Київський національний університет будівництва і архітектури, факультет автоматизації і інформаційних технологій, кафедра кібербезпеки та комп'ютерної інженерії, Київ, Україна

АНОТАЦІЯ

За допомогою хмарного сховища дані, такі як документи, файли, зображення та бази даних, передаються до хмарного сховища через підключення до інтернету, де зберігаються на віртуальних машинах у віддаленому фізичному центрі обробки даних. Щоб забезпечити доступність, безпеку та цілісність даних, хмарні сховища автоматично створюють резервні копії даних і зберігають копії даних на кількох машинах у географічно розкиданих місцях. Користувачі можуть отримати доступ до даних через інтернет-з'єднання практично на будь-якому пристрої.

Ключові слова

Хмарна система, система зберігання, файли, сервер, інформація.

Вступ

У сучасному інформаційному суспільстві, де обсяги даних стрімко зростають, питання ефективного та безпечного зберігання інформації стає ключовим. Хмарні сховища даних приходять на зміну традиційним локальним системам, пропонуючи революційні підходи до збереження та управління інформацією. Для зберігання даних використовуються сервери і системи зберігання даних, які фізично розташовані в географічно віддаленому від клієнта дата-центрі. Хмарне сховище - це структура розподілених у мережі онлайн-серверів, як правило, у вигляді онлайн-сервісу, що надає користувачам місце для зберігання їхніх даних. Сховище потрібно синхронізувати зі своїм пристроєм. Після цього туди можна завантажувати файли будь-якого типу. Вони будуть доступні з усіх пристроїв онлайн.

Основні визначення

Блочне сховище: Весь обсяг інформації ділиться на рівні частини - блоки з ідентифікаторами. Основна перевага таких хмарних сховищ - поділ клієнтських середовищ. Завдяки цьому до кожного з них відкривається швидкий окремий доступ. Але платити потрібно за весь виділений обсяг пам'яті, навіть якщо вона нічим не зайнята.

Файлове сховище: Дані зберігаються в ієрархічній системі. Це означає, що інформація являє собою файли, які об'єднуються в папки, підкаталоги і каталоги. Основна перевага - інтуїтивний інтерфейс і легкість використання. Головний

недолік - погана масштабованість: зі збільшенням обсягу даних ієрархія дуже сильно ускладнюється і уповільнює роботу системи.

Об'єктне сховище: Це універсальний і сучасний спосіб зберігання в хмарі великих інформаційних масивів. Об'єктне сховище використовується для даних будь-якого виду: медіаконтенту, програм, бухгалтерської/статистичної звітності тощо. Головний недолік - користувач не може просто взяти і перемістити файл у потрібну папку. Для завантаження інформації потрібно використовувати спеціальний програмний інтерфейс - API (він дає змогу двом незалежним компонентам ПЗ обмінюватися інформацією).

Результат дослідження

Існують сотні різних хмарних систем зберігання. Деякі з них мають дуже специфічну спрямованість, наприклад, зберігання повідомлень електронної пошти в Інтернеті або цифрових зображень. Інші доступні для зберігання всіх форм цифрових даних. Деякі хмарні системи зберігання даних є невеликими системами, тоді як інші настільки великі, що фізичне обладнання може заповнити цілий склад. Об'єкти, в яких розміщуються хмарні системи зберігання, називаються центрами обробки даних.

На найпростішому рівні хмарна система зберігання даних потребує лише одного сервера даних, підключеного до Інтернету. Клієнт (наприклад, користувач комп'ютера, який підписався на службу хмарного сховища) надсилає копії файлів через Інтернет на сервер, який записує інформацію. Коли клієнт бажає отримати інформацію, він отримує доступ до сервера даних через веб-інтерфейс. Потім сервер або надсилає файли назад клієнту, або дозволяє клієнту отримувати доступ до файлів на самому сервері та керувати ними.

Хмарні системи зберігання зазвичай покладаються на сотні серверів. Оскільки комп'ютери іноді потребують технічного обслуговування або ремонту, важливо зберігати однакову інформацію на кількох комп'ютерах. Це називається резервування. Без резервування хмарна система зберігання не могла б гарантувати клієнтам, що вони можуть отримати доступ до своєї інформації в будь-який момент часу. Більшість систем зберігають одні й ті ж дані на серверах, які незалежні одні від одного. Таким чином, клієнти можуть отримати доступ до своїх даних, навіть якщо один блок системи вийде з ладу.

Деякі з найбільш популярних хмарних сховищ для особистого використання та їх відмінності:

1. **Google Drive:**
   - Надає безкоштовний простір для зберігання файлів до 15 ГБ.
   - Має простий та інтуїтивно зрозумілий інтерфейс, а також численні інтеграції з іншими програмами Google, такими як Gmail, Google Docs та Google Sheets.

- Надає можливість спільної роботи над файлами та обміну ними з іншими користувачами.
- Забезпечує високу швидкість завантаження та скачування файлів.

2. Dropbox:

- Надає безкоштовний простір для зберігання файлів до 2 ГБ.
- Забезпечує високу швидкість завантаження та завантаження файлів, а також потужні можливості керування доступом до файлів.
- Має простий та інтуїтивно зрозумілий інтерфейс, а також численні інтеграції з іншими програмами та сервісами.
- Надає можливість спільної роботи над файлами та обміну ними з іншими користувачами.

3. Microsoft OneDrive:

- Надає безкоштовний простір для зберігання файлів до 5 ГБ.
- Забезпечує високий рівень безпеки та захисту даних, включаючи функцію захисту інформації та можливості керування доступом до файлів.
- Надає можливості для спільної роботи та обміну файлами за допомогою інтеграції з іншими програмами Microsoft, такими як Word, Excel та PowerPoint.
- Має простий та інтуїтивно зрозумілий інтерфейс.

4. iCloud:

- Надає безкоштовний простір для зберігання файлів до 5 ГБ.
- Забезпечує високий рівень безпеки та захисту даних, включаючи функцію двофакторної автентифікації.
- Має простий та інтуїтивно зрозумілий інтерфейс, а також інтеграції з іншими програмами Apple, такими як Pages, Numbers та Keynote.
- Надає можливості синхронізації даних між пристроями Apple.

Висновки

Одним із головних плюсів використання хмарних сховищ є підвищення доступності та віддаленості. За допомогою хмарного сховища ви можете отримати доступ до своїх даних з будь-якого місця і в будь-який час, якщо у вас є підключення до Інтернету. Це забезпечує гнучкість і зручність, особливо для тих, кому необхідно працювати віддалено або отримувати доступ до своїх файлів, перебуваючи в дорозі. Хмарне зберігання даних усуває необхідність у фізичній інфраструктурі зберігання. Вам не потрібно вкладати кошти в дороге обладнання і піклуватися про його обслуговування та підтримання в робочому стані. Це дає змогу заощадити час і гроші та забезпечити більш ефективне і масштабоване рішення для зберігання даних. Одним із недоліків хмарних сховищ є підвищена залежність від підключення до Інтернету. Без стабільного і надійного інтернет-з'єднання можуть виникнути труднощі з доступом до даних з хмари. Це може

завдати значних незручностей, особливо якщо доступ до даних необхідний у стислі терміни.

Література

[1] A Study on Data Storage Security Issues in Cloud Computing https://www.researchgate.net/publication/306071422_A_Study_on_Data_Storage_Security_Issues_in_Cloud_Computing.
[2] Data and Application Security in Cloud https://www.researchgate.net/publication/277603564_Data_and_Application_Security_in_Cloud.
[3] What is cloud storage https://www.ibm.com/topics/cloud-storage.

МЕДИЧНІ ДОДАТКИ ІНТЕРНЕТУ РЕЧЕЙ: ІННОВАЦІЇ У ВЕДЕННІ ЗДОРОВ'Я ТА ДІАГНОСТИЦІ ЗА ДОПОМОГОЮ ПРИСТРОЇВ

Євген НЮКАЛО (студент)

Київський національний університет будівництва і архітектури, факультет автоматизації і інформаційних технологій, кафедра кібербезпеки та комп'ютерної інженерії, Київ, Україна

Анотація

Доповідь розглядає вплив Інтернету речей (IoT) на медичні додатки та їхню роль у сучасній медицині. Зазначено, що підключені пристрої забезпечують неперервний моніторинг, точну діагностику та персоналізовані підходи до лікування. Обговорені виклики, такі як приватність даних та етичні аспекти, але висвітлено їхній потенціал для покращення охорони здоров'я та розвитку медичної практики.

Ключові слова

Медичні додатки інтернету речей, IoT, приватність даних, оптимізація.

Постановка задачі

Метою доповіді є дослідження впливу медичних додатків Інтернету речей (IoT) на сучасну медицину. Аналізуються можливості моніторингу здоров'я та покращення точності діагностики, враховуючи інноваційні технології, такі як сенсори та машинне навчання. Подається обговорення викликів, таких як приватність даних та безпека, і визначаються перспективи для подальшого розвитку. Задача полягає в системному дослідженні та об'єктивному викладенні інформації для надання комплексного розуміння цього питання.

Актуальність проблеми

Актуальність проблеми впровадження медичних додатків в сферу охорони здоров'я надзвичайно висока в сучасному світі. Зростання популяції, збільшення кількості пацієнтів з хронічними захворюваннями та потреба в ефективній медичній допомозі створюють тиск на сучасну систему охорони здоров'я.

Такі додатки можуть вирішити ці виклики, надаючи інструменти для неперервного моніторингу, ефективної діагностики та персоналізованого лікування. Підвищення доступності медичних послуг, зменшення витрат та покращення якості догляду за пацієнтами роблять цю технологію крайньою актуальною для подальшого розвитку сфери охорони здоров'я. Активний дослідницький інтерес та постійний технологічний прогрес підкреслюють важливість розгляду цієї проблеми.

Роль медичних додатків IoT у веденні здоров'я

Однією з ключових функцій медичних додатків IoT є можливість постійного моніторингу важливих вітальних показників, таких як пульс, артеріальний тиск та рівень кисню в крові. Сучасні підключені пристрої можуть автоматично відстежувати ці параметри, забезпечуючи постійний потік даних для аналізу стану здоров'я.

Медичні додатки IoT дозволяють не лише вимірювати важливі фізіологічні показники, але й вести облік фізичної активності та споживання калорій. Інтеграція цих даних дозволяє розробляти персоналізовані рекомендації щодо активності та життєвого стилю, що сприяє покращенню загального стану здоров'я.

Застосування IoT у сфері медицини дозволяє створювати системи нагадувань та контролю за прийомом ліків. Підключені пристрої можуть відстежувати вживання лікарств, повідомляти лікарів про можливі ускладнення та надавати пацієнтам рекомендації для забезпечення ефективного лікування.

Медичні додатки можуть інтегруватися з медичними інформаційними системами та електронними медичними картами. Це дозволяє лікарям та медичному персоналу отримувати доступ до актуальних даних пацієнта в режимі реального часу, полегшуючи прийняття рішень та надаючи більш інформовану медичну допомогу.

Зведення всіх цих даних в один інтегрований інтерфейс дозволяє створювати індивідуалізовані плани управління здоров'ям для кожного пацієнта. Інформаційна система може аналізувати дані та розробляти персоналізовані рекомендації щодо лікування та профілактики хвороб.

Інновації у діагностиці за допомогою підключених пристроїв

Медичні додатки IoT використовують різноманітні сенсори для збору об'єктивних даних, таких як температура, електрокардіограма, артеріальний тиск та рівень глюкози. Ці дані надходять в реальному часі, що дозволяє лікарям отримувати актуальну інформацію про стан пацієнта.

Розвиток технологій збору та передачі даних в реальному часі робить медичні дані доступними миттєво. Це особливо важливо для ефективного моніторингу та допомоги пацієнтам у випадках хронічних захворювань.

Використання аналітики даних та машинного навчання підвищує точність діагнозів, а автоматизовані системи моніторингу дозволяють підключеним пристроям вести неперервний контроль за станом хворого.

Системи електронних звітів та інтерактивна співпраця з пацієнтами роблять дані легко доступними та сприяють взаємодії між медичним персоналом і пацієнтами.

Виклики та перспективи впровадження медичних додатків

Важливим викликом є питання приватності даних. Зі збільшенням обсягу зібраних медичних даних виникає необхідність ефективної системи захисту конфіденційності, щоб запобігти неправомірному доступу.

Пристрої IoMT необхідно постійно перевіряти на безперебійну роботу та функціональність. Пристрій Інтернету речей, який має недоліки, може легко призвести до травм. Хоча деякі травми можуть бути незначними, інші можуть бути несприятливими. Ось чому медичні компанії Інтернету речей повинні стежити за тим, наскільки добре функціонують їхні пристрої..

Ще однією проблемою є забезпечення безпеки мережі та захист від кібератак. Зважаючи на чутливість медичних даних, їхнє збереження та передача повинні відповідати високим стандартам безпеки. Загроза безпеці, яку створюють пристрої IoMT, залежить від заходів безпеки виробника та кінцевого користувача. Недотримання нормативних вимог може зробити пристрої вразливими до порушень безпеки. Однак, навіть якщо виробник робить усе, щоб захистити пристрій - шифрування, управління патчами, і цілих дев’ять ярдів - безпека пристроїв все ще може бути порушена з боку користувача.

Етичні питання також є важливою частиною впровадження. Правильне використання даних та збереження приватності пацієнтів стає ключовими етичними аспектами, які вимагають уваги.

Несумісність технологій та відсутність стандартів можуть ускладнити взаємодію між різними системами медичних додатків IoT. Стандартизація інтерфейсів та протоколів взаємодії є важливим завданням для подальшого розвитку цих технологій.

З іншого боку, перспективи впровадження є великими. За допомогою цих технологій можна покращити доступність медичних послуг, зменшити витрати на лікування та підвищити ефективність медичного обслуговування. Також, інтеграція додатків такого типу з електронними медичними записами може полегшити обмін інформацією між медичними закладами та забезпечити більш координоване надання послуг.

Висновок

В заключенні, варто визначити, що медичні додатки представляють значущий потенціал для трансформації сучасної медицини та управління здоров'ям. Огляд використання підключених пристроїв вказує на їхню здатність забезпечувати неперервний моніторинг, точну діагностику та індивідуалізовані підходи до управління здоров'ям.

Медичні додатки IoT дозволяють створювати персоналізовані плани лікування та моніторингу, що в перспективі може покращити результати лікування

та якість життя пацієнтів. Сенсори, збору даних в реальному часі та аналітика допомагають лікарям приймати більш об'єктивні та оперативні рішення.

Однак їх впровадження не обійдеться без викликів. Питання приватності даних, безпеки мереж та етичних стандартів вимагають серйозної уваги та розв'язання. Стандартизація та узгодженість між різними системами також є критичними аспектами подальшого розвитку цих технологій.

Завдяки інноваційним можливостям, ці додатки вже вносять значущий вклад у покращення охорони здоров'я та стають ключовим фактором у розвитку сучасної медицини. Забезпечення балансу між високотехнологічними можливостями та ефективним управлінням викликами є важливою умовою для успішного впровадження цих технологій у медичну практику.

Усі ці аспекти вказують на те, що медичні додатки визначають новий етап у розвитку сфери охорони здоров'я. Настав час для глибшого розуміння та широкого обговорення цих технологій, щоб забезпечити їхню успішну інтеграцію у медичну практику та зробити значущий внесок у покращення якості медичної допомоги.

Література

[1] Журавель В.І., Ткачук Т.Ю., Борковський Д.С. Інтернет речей у системі медичної допомоги: можливості та безпека. Актуальні проблеми клініч. та профілакт. медицини. 2019. Т. 3, № 1/2. С. 5–12.

[2] Kyivstar: *https://hub.kyivstar.ua/articles/iot-u-medyczyni-vid-teoriyi-do-realnyh-kejsiv* , 01.02.2024.

[3] MOKO SMART: *https://www.mokosmart.com/uk/iot-medical-industry* , 03.02.2024

[4] Б.Ю. Жураковський, І.О. Зенів ТЕХНОЛОГІЇ ІНТЕРНТУ РЕЧЕЙ НАВЧАЛЬНИЙ ПОСІБНИК, С. 18-20.

[5] Б.Ю. ЖУРАКОВСЬКИЙ, І.О. ЗЕНІВ: Технології інтернету речей, навчальний посібник, Київ 2021.

[6] АНАЛИЗ ТРАФИКА УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ: *https://cyberleninka.ru/article/v/analiz-trafika-ustroystv-interneta-veschey*, 02.02.2024.

АНАЛІЗ ТЕХНОЛОГІЙ ДИСТАНЦІЙОГО КЕРУВАННЯ ЖИВЛЕННЯМ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ

Артем РАЙСЬКИЙ (студент)

Київський національний університет будівництва і архітектури, факультет автоматизації і інформаційних технологій, кафедра кібербезпеки та комп'ютерної інженерії, Київ, Україна
raijskijartemij@gmail.com

Анотація

Технологія Wake-On-LAN (WOL) в контексті мережевих середовищ є ключовим елементом для дистанційного управління та включення вимкнених пристроїв. У світлі широкого застосування цієї технології виникає важливе питання щодо забезпечення безпеки користувачів. Наводиться приклад побудови безпечної мережі для компенсації безпекових ризиків.

Wake-On-LAN (WoL) використовує спеціальний тип пакета, відомий як "Magic Packet" (чарівний пакет). Це унікальний мережевий пакет, що містить конкретну послідовність байтів. Для успішного включення в сплячий або вимкнений режим пристрою за допомогою WoL, Magic Packet розсилається в мережу. Пристрій, який підтримує WoL, впізнає цей спеціальний пакет і ініціює свій запуск.

Ключові слова

Керування живленням, мережа, енергозбереження, «розумний» будинок, безпека, локальна мережа, «Magic Packet».

Abstract

The Wake-On-LAN (WOL) technology in the context of network environments is a key element for remote control and activation of disabled devices. In light of the widespread use of this feature, there is an important question regarding the security of users. An example of building a secure network to compensate for security risks is given.

Keywords

Power Management, Network, Energy saving, Smart House, Security, Local Area Network, «Magic Packet».

Постановка проблеми

Wake-on-LAN – це технологія, яка покращить та оптимізує роботу систем, під'єднаних до однієї локальної мережі. Вона дозволяє віддалено керувати живленням комп'ютерів та серверів, виводячи систему з вимкненого або стану «у сні». Очікується, що в найближчі 5-10 років технологія буде вдосконалена, а саме алгоритм для використання (інтеграції) її в хмарні сервіси, та збільшення спектру її застосування в інших пристроях. В інфраструктуру входить множина автентифікованих пристроїв, таких як комп'ютери та сервери, що поєднані у мережу. Керуванням локальної мережі (LAN) займається Адміністратор. В найпростішому випадку це може бути проста програма, на якій зібрані показники

статусу пристрою та віджети для керування їх живленням для подальшого використання.

Ось деякі тенденції розвитку технології Wake-on-LAN, які можна передбачити вже зараз:

- Загальна тенденція розвитку WoL включає адаптацію до сучасних підходів до енергозбереження, таких як стандарти та ініціативи, спрямовані на зменшення витрат електроенергії..
- Нові можливості для WoL можуть включати підтримку високошвидкісного інтернету, адаптацію до нових мережевих технологій та інтеграцію з Інтернетом речей.
- Розробники можуть зосередитися на поліпшенні рівня безпеки WoL, використовуючи шифрування для захисту передачі даних та покращення процедур автентифікації для запобігання несанкціонованому доступу.
- Очікується, що WoL може бути інтегрований з хмарними сервісами, щоб забезпечити вдале управління пристроями та активацію їх в мережі через віддалений доступ.
- Орієнтація на розширення підтримки WoL для різноманітних пристроїв, таких як мультимедійні центри та смарт-пристрої, для більш широкого використання.
- Спроби встановлення єдиної стандартизації та протоколів для WoL з метою полегшення взаємодії між пристроями різних виробників та підвищення сумісності.

Впровадження WoL має не лише позитивний вплив, але й пов'язано з виникненням ризиків кібератак з витоком нешифрованого трафіку конфіденційних даних та перевантаженням пристроїв.
Ці проблеми потребують вирішення, як на технічному, так і на законодавчому рівні.

Мета доповіді

Метою доповіді є надання пропозицій щодо розв'язання перелічених проблем за рахунок впровадження технічних рішень, які дозволяють забезпечити захист системи WoL від проникнення.

Огляд та аналіз нормативних документів та стандартів щодо WoL

Для підтримки технологій WoL в галузі адміністрування розроблені наступні спеціальні стандарти:

- IEEE 802.3 Ethernet Standard: Стандарт IEEE 802.3, який регулює Ethernet, визначає фізичні та керуючі характеристики мережевого з'єднання. Він

включає аспекти, пов'язані з WoL, такі як керування енергоспоживанням та споживанням електроенергії.

- ACPI (Advanced Configuration and Power Interface): ACPI встановлює стандарти для керування енергоспоживанням та конфігурацією в сучасних комп'ютерах. WoL може використовуватися для взаємодії з ACPI для управління станом сну та енергозбереженням.
- Intel Wired for Management (WfM) Specification: Специфікація Intel WfM визначає стандарти для віддаленого керування та адміністрування комп'ютерами. WoL є однією з функцій, яку вона може підтримувати.
- Microsoft Wake-On-LAN Security Best Practices: Microsoft надає рекомендації щодо безпеки Wake-on-LAN, зокрема стосовно захисту від несанкціонованого доступу та використання шифрування для захисту передачі даних.
- ISO/IEC 27001 (Information Security Management System): Цей стандарт визначає вимоги до систем управління інформаційною безпекою. Врахування аспектів безпеки WoL може бути частиною стратегії управління інформаційною безпекою.
- Технічні характеристики від виробників обладнання: Багато виробників мережевого обладнання та комп'ютерів надають власні технічні характеристики та рекомендації для використання Wake-on-LAN на їхніх пристроях.

Ці стандарти визначають вимоги, архітектуру, протоколи та API для інтеграції технології в інфраструктуру розумних будівель, міст, тощо. Вони спрямовані на забезпечення сумісності, безпеки та надійного зв’язку між WoL пристроями.

Наведені стандарти закладають важливу основу для безпеки рішень Інтернету речей, але не можна сказати, що цього достатньо. Для комплексного забезпечення безпеки потрібен системний багатошаровий підхід, у відповідності до ризиків та критичності застосувань. Цей підхід має бути не тільки технічний, а й організаційний, в тому числі потрібно визначати вимоги до обслуговування, модернізації, ремонту, інтеграції зі штучним інтелектом, утилізації, копіювання, мінімальний рівень дублювання критичних підсистем, умови доступу правоохоронних органів, дозволені засоби захисту від втручань.

Отже, сучасні та майбутні стандарти закладають основу, але безпека – це комплексна предметна область, яка потребує особливої постійної уваги.

Пропозиції щодо впровадження безпечної мережі

Захист функції Wake-On-LAN (WOL) має важливе значення для запобігання можливим проблемам у сфері безпеки. Нижче подано кілька заходів, які можна прийняти для захисту WOL:

- Шифрування Трафіку: Використовуйте захищений протокол для WOL, такий як VPN або IPsec, щоб шифрувати трафік між пристроями та запобігти його перехопленню.
- Сегментація Мережі: Розміщуйте пристрої, що підтримують WOL, на окремих мережевих сегментах, щоб зменшити ризик від несанкціонованого використання.
- Використання Сильних Паролів: Задавайте сильні паролі для конфігурації WOL. Забезпечення безпеки паролів важливо для запобігання несанкціонованому доступу.
- Фільтрація MAC-Адрес: Встановлюйте фільтри MAC-адрес, щоб обмежити доступ до функції WOL лише для конкретних пристроїв у мережі.
- Відключення Функції Там, Де Непотрібно: Вимикайте функцію WOL на пристроях, якщо вона не використовується. Це допоможе уникнути потенційних загроз та зменшити ризик.
- Оновлення Прошивки: Регулярно оновлюйте прошивку пристроїв та маршрутизаторів для отримання останніх заходів безпеки, які можуть включати в себе покращення для функції WOL.
- Використання Внутрішніх Мережевих Механізмів Захисту: Використовуйте вбудовані механізми безпеки в мережевих пристроях, такі як файрволи, для контролю доступу до WOL.
- Моніторинг Логів: Активуйте моніторинг логів на мережевих пристроях для виявлення будь-яких невизначених або надто активних спроб використання WOL.

Застосування цих заходів допоможе покращити безпеку функції Wake-On-LAN та зменшити ризик потенційних загроз.

Висновки

Впровадження систем Wake-On-LAN (WoL) вносить новаторські підходи до вирішення базових завдань, але одночасно виникають проблеми, пов'язані з безпекою. Зловмисні втручання в роботу систем WoL можуть мати значно більший вплив порівняно із розрізненими випадками зловживань. Існуючі стандарти WoL визначають вимоги, архітектуру, протоколи та API для інтеграції цієї технології в інфраструктуру розумних будівель, підприємств та міст. Однак, забезпечення безпеки є складною предметною областю, яка вимагає постійної уваги.

У доповіді пропонуються технічні рішення для захисту мережі з технологією WoL від кібератак. Ці заходи безпеки спрямовані на зменшення ризиків та ефективний контроль за можливими загрозами безпеки в контексті використання WoL в різних сферах, таких як розумні будівлі, підприємства та міські інфраструктури.

Література

[1] "Understanding 802.1X Authentication with Wake-on-LAN": https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dot1x.html#wp1133592.
[2] White Paper: Wake on LAN Technology by Lieberman Software Corporation. Rev 2 – June 1, 2006: https://elielecatportefoliosio.files.wordpress.com/2016/04/wake_on_lan.pdf.
[3] White Paper: "Magic Packet Technology" AMD. November 1995.: https://web.archive.org/web/20141006072000/http://support.amd.com/TechDocs/20213.pdf.
[4] "'Wake on LAN' (WOL) behavior in Windows 10" Microsoft. April 2023: https://learn.microsoft.com/en-US/troubleshoot/windows-client/deployment/wake-on-lan-feature.
[5] "Understanding Wake On LAN". LANdesk.com. Retrieved 28 October 2015: https://forums.ivanti.com/s/article/Understanding-Wake-On-LAN?language=en_US.

ОПТИМІЗАЦІЯ ІНТЕГРАЦІЇ ДАНИХ ДЛЯ ЕКОСИСТЕМ SMART ІНДУСТРІЇ: ВИКОРИСТАННЯ ВЕБ-РОЗРОБКИ, БАЗ ДАНИХ ТА ХМАРНИХ СХОВИЩ

Сергій ЧАЮК (студент)

Київський національний університет будівництва і архітектури, факультет автоматизації і інформаційних технологій, кафедра кібербезпеки та комп'ютерної інженерії, Київ, Україна

Анотація

Smart індустрія, що розвивається, характеризується великою кількістю взаємопов'язаних пристроїв, які створюють величезну кількість різноманітних даних. Ефективна інтеграція та аналіз цих даних мають вирішальне значення для оптимізації операцій і прийняття рішень. У цій роботі розглядається, як веб-розробка, бази даних і хмарне сховище можуть разом вирішити цю проблему.

Потік даних у Smart індустрії

Smart індустрія, або Індустрія 4.0, знаменує собою нову еру виробництва, де бурхливо зростає автоматизація традиційних і виробничих практик з використанням сучасних інтелектуальних технологій [1]. Ця трансформація ґрунтується на зборі, обробці та аналізі величезних обсягів даних, що генеруються протягом усього виробничого ланцюжка.

Smart індустрія переповнена різноманітними даними, від показань датчиків і виробничих показників до відстеження логістичного забезпечення та взаємодії споживачів. Дані є багатогранними, вони дають важливу інформацію про стан обладнання, ефективність роботи, динаміку ланцюга поставок і прийняття стратегічних рішень. Розуміння цього різноманіття має важливе значення для ефективного управління даними.

Робота з таким обсягом та різноманіттям даних призводить до ряду проблем:

- Неоднорідність даних: уніфікація різноманітних форматів, структур і джерел є значною перешкодою.
- Обробка в реальному часі: динамічний характер Smart індустрії потребують обробки в реальному часі для прийняття оперативних рішень.
- Питання безпеки: захист конфіденційної інформації від злому та несанкціонованого доступу має першочергове значення.

Вирішення цих проблем потребує технологій і стратегій, які працюватимуть узгоджено. Здатна це забезпечити автоматизована система, побудована з використанням сучасних інструментів. Для реалізації такої системи існує безліч варіантів, але одним із найефективніших є застосування веб-технологій з використанням баз даних та хмарного сховища, які разом забезпечать гнучкість, доступність і захист системи.

Веб-розробка для Smart індустрії

Різноманіття пристроїв та джерел даних, які в свою чергу можуть спілкуватися між собою різними мовами в екосистемі Smart індустрії, робить інтеграцію та обмін даними складним завданням. В подоланні цього розриву ключовим фактором можуть стати API та веб-фреймворки.

Уявіть собі універсальний перекладач, який передає інформацію між пристроями незалежно від їхньої рідної мови, в цьому сила API. API (Application Programming Interface) – це стандартизований інтерфейс, який дозволяє програмам обмінюватися даними [2]. Веб-API використовують декілька протоколів, але з них RESTful API є найпоширенішим типом API, пропонуючи набір чітко визначених методів для доступу до даних, таких як GET, POST, PUT та DELETE [3][4].

Завдяки стандартизації, безперебійному зв'язку, масштабованості та гнучкості API роблять інтеграцію даних значно простішою, що веде до кращого використання даних та прийняття більш обґрунтованих рішень.

Веб-фреймворки здатні допомогти у створенні інфраструктури для плавного обміну даними. Популярні фреймворки, як Django або Spring, пропонують готові інструменти та функції для створення надійних API, що дозволяє розробникам зосередитися на конкретних потребах програми Smart індустрії.

Сучасні фреймворки, такі як Angular, React та Vue.js, пропонують потужні інструменти для створення інтерфейсів користувача, які можуть візуалізувати дані з різних джерел [5]. Ці фреймворки роблять акцент на модульності, повторному використанні компонентів та односторінкових додатках (SPA), що забезпечує гнучкість та масштабованість при розробці складних веб-додатків.

Іноді системі потрібна інформація якої немає у внутрішній мережі, а є у зовнішніх джерелах, наприклад ринкові тенденції чи настрої в соціальних мережах. Для такого існує веб-скрапінг – метод збору даних з веб-сайтів. Цей метод може бути корисним для доступу до даних, які не доступні через API.

Можна сказати, що інструменти веб-розробки діють як міст та інтерпретатор, долаючи розрив між різними пристроями та джерелами даних в екосистемі Smart індустрії.

Бази даних для структурованої та неструктурованої інформації

Розумна галузь створює масу даних, починаючи від структурованих виробничих параметрів і закінчуючи неструктурованими показаннями датчиків [6]. Для зберігання та обробки цих даних потрібні відповідні бази даних. Вибір правильного рішення для зберігання даних вимагає орієнтації на сильні та слабкі сторони двох ключових конкурентів баз даних: реляційні та NoSQL.

Реляційні бази даних, такі як MySQL, PostgreSQL та Oracle, добре підходять для структурованих даних, які мають чітко визначену структуру та схему. Ці дані організовані в таблиці, що складаються з рядків і стовпчиків.[7]

Бази даних NoSQL, такі як MongoDB, Cassandra та HBase, розроблені для неструктурованих даних, які не мають чіткої структури. Ці дані можуть зберігатися у форматі JSON, XML, або просто у текстовому форматі.[8]

Самі по собі реляційні і NoSQL бази даних не пропонують ідеального рішення для зберігання та обробки даних. Але існує гібридний підхід, який використовує обидві технології. Використовуючи сильні сторони кожного типу бази даних, можна створювати більш цілісну систему керування даними.

Ідея гібридного підходу полягає в наступному:

- Структуровані дані , такі як виробничі параметри та фінансові записи, можуть комфортно розміщуватися в реляційних базах даних, виграючи від їхніх ефективних запитів і функцій цілісності даних.
- Неструктуровані та напівструктуровані дані, такі як показання датчиків і взаємодії з соціальними мережами, можна зберігати в базах даних NoSQL, де їх гнучкість забезпечує різноманітні формати та динамічні схеми.

Інструменти інтеграції даних сприяють безперебійному обміну даними між цими розрізненими базами даних, забезпечуючи уніфікований доступ і аналіз у всьому ландшафті даних. Цей гібридний підхід сприяє гнучкості, ефективності та масштабованості, ключовим аспектам для управління постійно зростаючими вимогами до даних інтелектуальної промисловості.

Загалом вибір бази даних залежить від вимог системи, характеристики даних і загальної архітектури системи, адже використання універсального рішення може бути не ефективним в конкретній ситуації.

Перевага хмари для масштабованості та співпраці

Smart індустрія процвітає завдяки даним, тому зберігання та керування ними важливий фактор, який впливає на роботу системи. Обробка даних в рамках локальної інфраструктури може бути не ефективною і в перспективі призвести до проблем. Тому хмарні технології стають все більш важливим фактором для успішного впровадження Smart індустрії. Хмарні рішення для зберігання даних пропонують ряд переваг з точки зору масштабованості, безпеки, доступності та співпраці, що робить їх ідеальними для роботи з великими обсягами даних, які генеруються в екосистемах Smart індустрії.

Уявіть оркестр, який може миттєво додавати або видаляти інструменти за потреби, так само хмарне сховище здатне динамічно збільшити або зменшити обсяг пам’яті, адаптуючись до коливань обсягів даних у режимі реального часу [9]. Це дозволяє підприємствам легко справлятися з піковими навантаженнями та економити кошти на ресурсах, які не використовуються.

Зберігання даних у хмарних сховищах гарантує безпеку завдяки сучасним та надійним засобам захисту, таких як шифрування, контроль доступу, багатофакторна автентифікація, моніторинг безпеки, вдосконалені системи виявлення вторгнень тощо [10].

Хмарні бази даних доступні з будь-якого місця і будь-якого пристрою, що робить дані доступними для всіх зацікавлених сторін в екосистемі – від інженерів до аналітиків і керівників, сприяючи прийняттю важливих рішень і спрощеній співпраці, незалежно від їхнього розташування [11].

Хмарні платформи також дозволяють проводити аналітику в реальному часі, що дає можливість підприємствам отримувати цінні статистичні відомості з даних Smart індустрії та приймати більш обґрунтовані рішення [12].

Вказані можливості вже роблять хмару популярним рішенням для зберігання та обробки даних, але це тільки основне. Хмарні сховища здатні забезпечити безперебійність роботи навіть у непередбачених обставинах, а також не менш важливе резервне копіювання.

Висновок

Ефективне керування даними є ключовим фактором успішного впровадження екосистеми Smart індустрії. Веб-розробка, бази даних і хмарне сховище відіграють важливу роль в оптимізації інтеграції даних.

Фреймворки та API роблять дані доступними з будь-якого пристрою та забезпечують безперебійний зв'язок, бази даних дають можливість зберігати та обробляти різні типи даних, а хмарне сховище пропонує масштабованість, безпеку, доступність та аналітику в реальному часі, тощо.

Набір цих інструментів вже робить побудовану систему потужним рішенням, але прогрес не стоїть на місці і кожен день з’являється все більша кількість підключених до Інтернету пристроїв, що призводить до ще більшого зростання обсягів даних і очевидно потребує нових рішень в покращення або доповнення існуючої можливості керування даними. Потенційно, одним із таких може бути штучний інтелект і машинне навчання, широко відомі сьогодні, які можуть автоматизувати прийняття рішень, дати змогу глибше аналізувати дані на основі передбачених результатів та майбутніх тенденцій, тощо.

Література

[1] Чому так важлива четверта промислова революція? Розбираємося в технологіях індустрії 4.0 – ID Card URL: https://idcard.com.ua/ua/blog/why-is-the-fourth-industrial-revolution-so-important/.

[2] Що таке API: простими словами про складне – Host IQ URL: https://hostiq.ua/blog/ukr/what-is-api/.

[3] 3 API Protocol Types: Their Differences and When To Use Each – getstream URL: https://getstream.io/blog/api-protocols.

[4] Вступ до REST API — RESTful вебсервіси – r_d media URL: https://robotdreams.cc/uk/blog/466-vstup-do-rest-api-restful-vebservisi.
[5] Front-end фреймворки: Використання React, Angular або Vue.js – IT Рейтинг україни URL: https://it-rating.ua/front-end-freymvorki-vikoristannya-react-angular-abo-vuejs.
[6] Empowering Smart Factories: Unveiling 5 Invaluable Data Management Tips for Achieving Ultimate Success. – Data Dynamics URL: https://www.datadynamicsinc.com/blog-empowering-smart-factories-5-data-management-tips-for-ultimate-success.
[7] Реляційні бази даних усе, що необхідно про них знати – foxminded URL: https://foxminded.ua/reliatsiini-bazy-danykh.
[8] Характеристики NoSQL баз даних – javarush URL: https://javarush.com/ua/quests/lectures/ua.questhibernate.level19.lecture01.
[9] Хмарні бази даних. Детальна інструкція, як застосовувати сучасний IT-підхід – DOU URL: https://dou.ua/forums/topic/43820.
[10] Як хмарні технології захищають бізнес-дані – URL: https://mklegalservice.com/tpost/ry4bxvj9t1-yak-hmarn-tehnolog-zahischayut-bznes-dan.
[11] Що таке хмарні технології? Переваги та недоліки хмарних сервісів – edin URL: https://edin.ua/shho-take-xmarni-texnologi%D1%97-i-navishho-voni-potribni.
[12] Хмарні інструменти у цифровому маркетингу – APIXDrive URL: https://apix-drive.com/ua/blog/marketing/hmarni-instrumenti-u-cifrovomu-marketingu.

ЛЮДСЬКИЙ ФАКТОР В БЕЗПЕЦІ IoT

Ігор ОВЧАРУК (студент)

Київський національний університет будівництва і архітектури, факультет автоматизації і інформаційних технологій, кафедра кібербезпеки та комп'ютерної інженерії, Київ, Україна

Анотація

В сучасному цифровому світі, де Internet of Things (IoT) стає невіддільною частиною нашого повсякденного життя, виникає необхідність докладного вивчення безпеки цієї технологічної еволюції. Серйозний аспект цієї безпеки, який, можливо, не отримує достатньо уваги, але має критичне значення, - це взаємодія людини з IoT системами.

У цьому контексті, викриття користувачів до ризиків та їхнє розуміння можуть значно впливати на загальний рівень безпеки в цифровій екосистемі. Цей пункт статті спрямований на розгляд важливості розуміння людського фактора в контексті безпеки IoT.

Ми дослідимо, як відношення користувачів до ризиків визначає їхню поведінку в екосистемі IoT, яка може мати величезний вплив на загальний рівень загроз та вразливостей. Також буде розглянуто психологічні аспекти, пов'язані зі сприйняттям ризиків та впливом соціокультурних чинників на взаємодію людей з IoT пристроями.

Розуміння цих аспектів є критичним для розробки ефективних стратегій забезпечення безпеки в області IoT та врахування потреб та перспектив користувачів у цьому динамічному та швидкому сегменті технологій.

Ключові слова

Кібербезпека, людський фактор, аутентифікація, шифрування, стандарти безпеки, соціальна інженерія.

Annotation

In today's digitalized world, where the Internet of Things (IoT) is becoming an integral part of our daily lives, there is a need to examine the security of this technological evolution in detail. A serious aspect of this security that may not receive enough attention, but is of critical importance, is human interaction with IoT systems.

In this context, user exposure to and understanding of risks can have a significant impact on the overall level of security in the digital ecosystem. This section of the paper aims to address the importance of understanding the human factor in the context of IoT security. We will explore how users' attitudes toward risk determine their behavior in the IoT ecosystem, which can have a huge impact on the overall level of threats and vulnerabilities. We will also look at psychological aspects related to risk perception and the impact of socio-cultural factors on people's interaction with IoT devices.

Understanding these aspects is critical to developing effective IoT security strategies and taking into account the needs and perspectives of users in this dynamic and fast-paced technology segment.

Keywords

Cyber security, human factors, authentication, encryption, security standards, social engineering.

Постановка задачі

Однією з ключових областей дослідження в контексті безпеки Internet of Things (IoT) є ретельний аналіз взаємодії людини з цією технологічною екосистемою. У цій тезі буде зосереджено увагу на висвітленні сучасних досліджень та виявленні факторів, які визначають, як користувачі взаємодіють з IoT системами, включаючи пристрої, платформи та інтерфейси.

Аналізуючи літературні дані, буде розглянуто типові сценарії використання IoT, визначено основні виклики, які можуть виникнути в процесі взаємодії, та оброблено, які чинники можуть впливати на загальний рівень безпеки. Особлива увага буде приділена розробленню та використанню інтерфейсів, які враховують психологічні особливості користувачів, спрощуючи їхнє взаємодію з IoT пристроями та забезпечуючи високий рівень безпеки в цьому контексті.

Людський фактор у використанні IoT

З огляду на стрімкий розвиток технологій Internet of Things (IoT), питання безпеки виникає як один з найактуальніших викликів для розгляду. Розширення мережі підключених пристроїв призводить до збільшення обсягу обміну даними, що викликає неабиякі труднощі в забезпеченні конфіденційності та цілісності інформації[1].

Зростання важливості безпеки в IoT-додатках зумовлено кількома чинниками. По-перше, велика кількість пристроїв, які взаємодіють у цих мережах, створює широкий вектор можливих атак. Кіберзлочинці можуть використовувати слабкі точки в безпеці одного пристрою для потрапляння в інші елементи системи.

По-друге, великий обсяг збирання та обміну особистої інформації через IoT може призвести до серйозних порушень конфіденційності. Захист особистих даних користувачів стає вельми важливим завданням, оскільки недостатній рівень безпеки може призвести до непередбачених наслідків, включаючи крадіжку ідентичності та несанкціонований доступ до особистої інформації.

Таким чином, забезпечення безпеки в IoT-додатках стає необхідною умовою для збереження довіри користувачів, стійкості систем та успішного розвитку цієї перспективної галузі технологій[1].

Вплив людського фактора на безпеку мережевих пристроїв визначається різноманіттям чинників. Поведінка користувачів, їхні уподобання та навички використання технологій, а також ставлення до аспектів безпеки грають важливу роль.

Насамперед використання слабких паролів або їхнє використання на декількох пристроях може становити загрозу безпеці. Аутентифікація двома чинниками може служити ефективним рішенням для забезпечення додаткового рівня захисту.

Питання оновлення програмного забезпечення також важливе. Відкладання або ігнорування оновлень може призвести до вразливостей у системі.

Соціальна інженерія, така як фішинг, може використовуватися для обману користувачів та отримання конфіденційної інформації.

Поведінка користувачів, зумовлена їхнім рівнем усвідомленості та розумінням ризиків, може впливати на безпеку використання мережевих пристроїв.

Дизайн інтерфейсів та їхня зручність також грають важливу роль. Зручний та зрозумілий інтерфейс може сприяти правильному використанню, тоді як неякісний дизайн може призвести до помилок та непорозуміння.

Вплив людського фактора на безпеку мережевих пристроїв може бути зменшений шляхом підвищення усвідомленості користувачів, застосування технологій безпеки та створення зручних інтерфейсів. Освіта та навчання грають ключову роль у зменшенні впливу людського фактора на вразливість мережевих пристроїв.

У той час, коли ретельно пророблені інструменти, технології та функції є критичними для забезпечення кібербезпеки, вони залишаються неефективними у вирішенні того, що вважається слабким місцем в цьому контексті: людським фактором.

Саме тому для підприємств важливо встановлювати та застосовувати стандарти, дотримуватися політик у своїх рішеннях і впроваджувати правила, які забезпечують дотримання передового досвіду в межах компанії. Це включає рекомендації щодо підключення особистих пристроїв до мережі, таких як смартфони чи точки бездротового доступу.

З такими докладними знаннями про обладнання та пристрої в мережі, підприємства можуть розробити процеси та процедури для захисту. Це, в свою чергу, забезпечує, що пристрої мають відповідні функції безпеки та можуть бути посилені чи оновлені за допомогою прошивки.

Після введення правил в дію для підприємства також важливо мати довірену особу, яка взаємодіє з IT-правилами та співпрацює з інтегратором для переконання у відповідності пристроїв цим вимогам. Наприклад, однією з політик може бути вимога, щоб будь-який пристрій, підключений до мережі (відеореєстратор, робоча станція або система відеоспостереження), обмінювався даними за допомогою шифрування в локальній мережі клієнта, з метою зниження ризику кібератак.

Згідно з цією політикою будь-яка встановлена IP-камера має включати шифрування, а програмне забезпечення для відеоспостереження повинно бути здатним зчитувати зашифровані повідомлення з цієї камери. Крім того, кінцеві користувачі повинні бути уважні при використанні смартфонів і застосовувати правила, що захищають мережу підприємства від можливого вторгнення за допомогою особистих пристроїв окремих користувачів.

Висновки

У висновку можна констатувати, що несвідоме та неправильне користування мережевими пристроями є важливим аспектом, що визначає загрози в галузі безпеки Internet of Things (IoT). Згідно з аналізом впливу людського фактору, виявленого у цьому діалозі, ключовими викликами є використання слабких паролів, недостатня усвідомленість користувачів, і соціальна інженерія.

Для подолання цих викликів, важливо встановлювати стандарти та політики безпеки, які регулюють використання мережевих пристроїв. Крім того, освіта та навчання користувачів є ключовим елементом у зменшенні вразливості системи перед людським фактором.

Технологічні рішення, такі як використання аутентифікації двома чинниками та розвиток шифрування, визначаються як ефективні заходи безпеки. Аналіз сучасних викликів та перспектив розвитку заходів безпеки IoT підкреслює необхідність постійного вдосконалення стратегій у цьому напрямку.

Залучення довіреної особи та співпраця з інтеграторами також визначаються як важливі для ефективного впровадження правил та політик безпеки в організації.

Усі ці аспекти спільно спрямовані на подолання людського фактору та створення стійкого середовища для безпеки IoT. Остаточно, розуміння та врахування впливу людського фактору є критичними для розвитку ефективних стратегій безпеки в епоху зростаючої важливості Internet of Things.

Література

[1] Електронне джерело: Безпека IoT-рішень підприємств. Доступ: https://worldvision.com.ua/bezopasnost-iot-resheniy-predpriyatiy/.

ОЦІНКА АНАЛІЗ БЕЗПЕКИ В ДОДАТКАХ ДЛЯ IoT

Ігор ОВЧАРУК (студент)

Київський національний університет будівництва і архітектури, факультет автоматизації і інформаційних технологій, кафедра кібербезпеки та комп'ютерної інженерії, Київ, Україна

Анотація

Здатність розумних об'єктів залишатися на зв'язку з Інтернетом з метою передачі та отримання даних називається Інтернет речей (IoT). Згідно з останніми оцінками, до 2020 року кількість IoT-пристроїв перевищить 50 мільярдів. Не дивно, що таке стрімке зростання кількості IoT-пристроїв привертає увагу зловмисників, які прагнуть увагу зловмисників, які прагнуть використати їх для власної вигоди. власної вигоди, а ботнет Mirai є, мабуть, найбільш яскравим прикладом шкідливого програмного забезпечення, орієнтованого на IoT [1, 2]. По суті, IoT несе з собою безліч потенційних ризиків для безпеки і конфіденційності для кінцевих користувачів, включаючи несанкціонований доступ і зловживання приватною інформацією, а також зловживання приватною інформацією, уможливлення та посилення атак на інші системи, а також створення ризиків що стосуються особистої безпеки [3]. Зокрема, IoT сприяє створенню різноманітних ризиків для приватності споживача пов'язаних зі збором особистої та конфіденційної інформації, наприклад, про вподобання, місцезнаходження, звички тощо. У середньостроковій або довгостроковій перспективі ці дані можуть бути використані, скажімо, для створення профілю або видачі себе за користувача чи групу осіб, які його цікавлять. З іншого боку, такі ризики для безпеки, конфіденційності та довіри можуть значно зменшити довіру кінцевих користувачів до Інтернету речей, а отже, перешкоджати його повній реалізації.

Ключові слова

Internet of Things (IoT), безпека в IoT, аналіз безпеки, шифрування в IoT, виклики безпеки в IoT

Annotation.

The article "Security in Applications for the Internet of Things (IoT): Analysis, Challenges, and Innovations" provides an in-depth look at the key aspects of security in the development and use of IoT applications. Starting with an analysis of the current state of the IoT industry, the author discusses the importance of protecting information, operating systems, and database organisation in this context.

Aimed at identifying the technological challenges faced by developers and users of IoT applications, the article analyses the concept of information security from authentication and authorisation to encryption and protection against data interception. The ethical aspects and the impact of IoT on the economy and industry are considered, and the importance of innovative approaches to security in IoT applications is emphasised.

Using an analytical approach and evidence-based thinking, the article reveals the prospects and challenges facing developers and users in today's IoT world.

Keywords

Internet of Things (IoT), security in IoT, security analysis, encryption in IoT, security challenges in IoT

Постановка задачі

Internet of Things (IoT) представляє собою мережу фізичних пристроїв, обладнаних сенсорами, програмним забезпеченням та іншими технічними засобами для збору та обміну даними через Інтернет. У сучасному світі IoT відіграє ключову роль у підключенні різноманітних пристроїв та систем, що дозволяє забезпечувати автоматизацію, збільшувати ефективність та полегшувати повсякденне життя.

IoT знаходить застосування в різних галузях, включаючи медицину, промисловість, сільське господарство та побутові потреби. За допомогою сенсорів та з'єднання з хмарними системами, пристрої IoT можуть збирати та обробляти величезний обсяг даних для надання корисної інформації та управління різними аспектами виробництва та повсякденного життя.

Розуміння сутності та ролі IoT є ключовим для дослідження та забезпечення його безпеки, оскільки розвиток цієї технології вимагає ефективних заходів для захисту від потенційних загроз та атак.

Актуальність проблеми

З огляду на стрімкий розвиток технологій Internet of Things (IoT), питання безпеки виникає як один з найактуальніших викликів для розгляду. Розширення мережі підключених пристроїв призводить до збільшення обсягу обміну даними, що викликає неабиякі труднощі в забезпеченні конфіденційності та цілісності інформації.

Зростання важливості безпеки в IoT-додатках зумовлено кількома чинниками. По-перше, велика кількість пристроїв, які взаємодіють у цих мережах, створює широкий вектор можливих атак. Кіберзлочинці можуть використовувати слабкі точки в безпеці одного пристрою для потрапляння в інші елементи системи[1].

По-друге, великий обсяг збирання та обміну особистої інформації через IoT може призвести до серйозних порушень конфіденційності. Захист особистих даних користувачів стає вельми важливим завданням, оскільки недостатній рівень безпеки може призвести до непередбачених наслідків, включаючи крадіжку ідентичності та несанкціонований доступ до особистої інформації.

Таким чином, забезпечення безпеки в IoT-додатках стає необхідною умовою для збереження довіри користувачів, стійкості систем та успішного розвитку цієї перспективної галузі технологій.

Загрози конфіденційності

Забезпечення конфіденційності в системах Internet of Things (IoT) є надзвичайно важливим аспектом з огляду на обмін великими обсягами чутливої інформації між підключеними пристроями. Розглянемо деякі з основних загроз для конфіденційності в IoT:

- Перехоплення даних: Зловмисники можуть використовувати різноманітні методи для перехоплення інформації, що передається між пристроями IoT. Це може включати атаки на безпеку мережі, використання методів аналізу трафіку або навіть фізичний доступ до пристроїв.
- Несанкціонований доступ: Загрози з боку хакерів можуть призвести до несанкціонованого доступу до пристроїв IoT та злому систем аутентифікації. Це може використовуватися для отримання конфіденційної інформації або впливу на роботу пристроїв.
- Маніпулювання даними: Атаки на цілісність даних можуть призвести до внесення змін у передані дані, що може викликати неправильну роботу пристроїв або спричинити негативні наслідки.
- Виток інформації про користувача: У випадку, коли пристрої IoT збирають особисті дані користувачів, існує ризик, що ця інформація може стати об'єктом витоку. Це може виникнути через слабкість заходів безпеки на рівні пристроїв або в мережевому середовищі.

Важливість конфіденційності визначається потребою забезпечити захист чутливої інформації, яка передається між підключеними пристроями. Ризики для конфіденційності включають можливість перехоплення даних, несанкціонований доступ, маніпулювання даними та виток особистої інформації користувачів[1].

Захист доступу в IoT визначається необхідністю контролювати, хто має право взаємодіяти з підключеними пристроями. Ризики, пов'язані із захистом доступу, включають слабку аутентифікацію, використання стандартних облікових записів, нестійкість алгоритмів аутентифікації та неадекватне управління правами доступу.

Для забезпечення безпеки в цих областях важливо використовувати ефективні механізми шифрування, сильну аутентифікацію, регулярно змінювати паролі та надавати тільки необхідні права доступу. Такий підхід допомагає зменшити ризики несанкціонованого доступу та зберегти конфіденційність інформації в системах IoT.

Критичний огляд засобів безпеки, використовуваних у сучасних IoT-додатках

У контексті Internet of Things (IoT), аутентифікація та авторизація є важливими складовими для забезпечення безпеки пристроїв та мережі.

Аутентифікація є процесом перевірки ідентичності користувача або пристрою перед наданням доступу до системи. У випадку IoT це може включати в себе використання паролів, біометричних даних, токенів або інших методів. Проблеми аутентифікації можуть виникнути внаслідок слабких паролів, витоків облікових даних або атак на процес аутентифікації.

Авторизація визначає, які дії та ресурси має право виконати аутентифікований користувач чи пристрій. Важливо дотримуватися принципу "не більше прав, ніж потрібно", щоб уникнути несанкціонованого використання пристроїв чи доступу до конфіденційної інформації. Проблеми авторизації можуть виникнути через неправильно налаштовані права доступу або вразливості в системі управління доступом[2].

Міцність системи аутентифікації та авторизації важлива для запобігання несанкціонованого доступу, захисту від атак та забезпечення цілісності даних. Ефективна реалізація цих механізмів допомагає зменшити ризики злому безпеки в IoT-додатках та підтримує стійкість систем у вимірі доступу до ресурсів.

У сучасних системах Internet of Things (IoT), де дані активно обмінюються між підключеними пристроями, захист від перехоплення даних та шифрування відіграють ключову роль в забезпеченні безпеки.

Шифрування - це процес перетворення інформації в такий формат, що його важко чи навіть неможливо розшифрувати без наявності спеціального ключа. У випадку IoT, шифрування може використовуватися для захисту переданих даних між пристроями від несанкціонованого доступу або перехоплення.

Цей аспект включає в себе заходи, спрямовані на попередження атак, спрямованих на зловживання або перехоплення передаваних даних. Використання захищених мережевих протоколів, таких як HTTPS, та механізмів ідентифікації може допомогти уникнути проблем з перехопленням інформації.

Міцне шифрування та захист від перехоплення даних є важливими, оскільки забезпечують конфіденційність та цілісність інформації в мережі IoT. Проте, важливо постійно оновлювати та вдосконалювати заходи безпеки, оскільки техніки атак швидко еволюціонують, і слабкість у захисті може призвести до непередбачених наслідків.

Перспективи розвитку безпеки в додатках для IoT

В контексті постійного вдосконалення безпеки в Internet of Things (IoT) важливо враховувати новаторські підходи. Один із таких підходів - використання технології блокчейн для створення безпечних та невід'ємних систем збереження даних. Ця технологія дозволяє створювати розподілені бази даних, що забезпечують цілісність та надійність інформації.

Також, використання систем машинного навчання може допомогти виявляти аномалії в роботі IoT-додатків, забезпечуючи більш ефективний моніторинг безпеки та реагування на потенційні загрози. Ще один підхід - застосування

технологій "захисту від кінцевого до кінцевого", який передбачає захист інформації на всіх етапах передачі, забезпечуючи повну безпеку даних від сенсора до цільової системи.

Забезпечення етичності та прозорості в розробці та використанні додатків для Internet of Things (IoT) є ключовим аспектом в сучасному цифровому середовищі.

З ростом кількості підключених пристроїв та збільшенням обсягу зібраної інформації, виникають питання етики використання цих даних. Розробники та користувачі повинні ретельно розглядати, як збирати, зберігати та використовувати особисті дані, щоб уникнути порушень приватності та неправильного використання інформації[2].

Прозорість визначається як здатність розуміти, як працює система та як обробляється інформація. В контексті IoT, це означає, що користувачі та інші зацікавлені сторони повинні мати чітке уявлення про те, як збираються та використовуються їхні дані, а також як працюють підключені пристрої.

Етична розробка та використання додатків для IoT допомагає зберегти довіру користувачів та уникнути можливих етичних конфліктів. Розробники повинні дотримуватися стандартів конфіденційності та прозорості, а також активно співпрацювати з органами регулювання для встановлення та дотримання етичних стандартів у галузі IoT.

Висновки

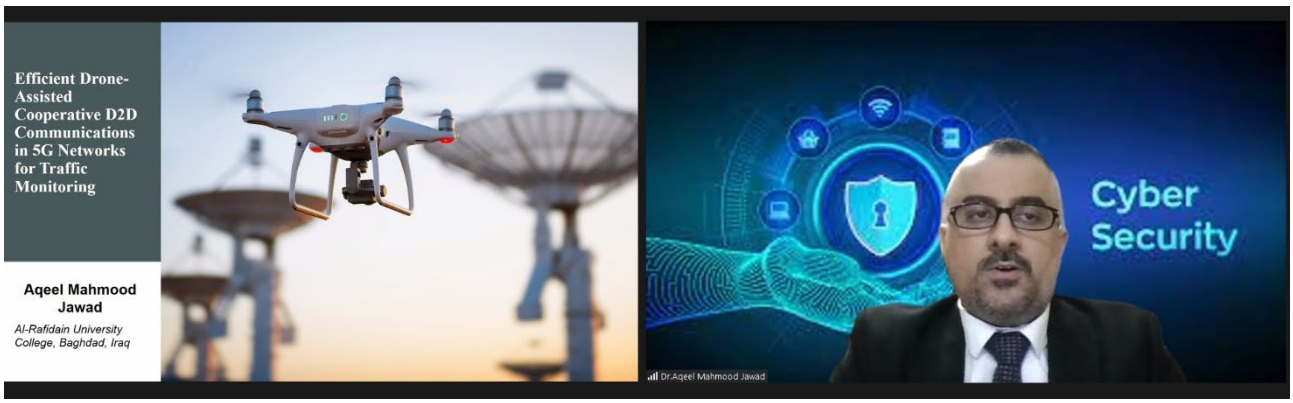
Вплив Internet of Things (IoT) на економіку та індустрію визначається кількома ключовими аспектами. Спочатку, використання IoT у виробництві призводить до підвищення ефективності та автоматизації процесів, забезпечуючи економію ресурсів. Другий аспект полягає в розвитку нових ринків через створення нових продуктів та послуг, таких як розумні домашні пристрої та медичні технології. Третій аспект включає розвиток підприємництва, де підприємства, активно використовуючи IoT, можуть створювати нові бізнес-моделі та привертати інвестиції.

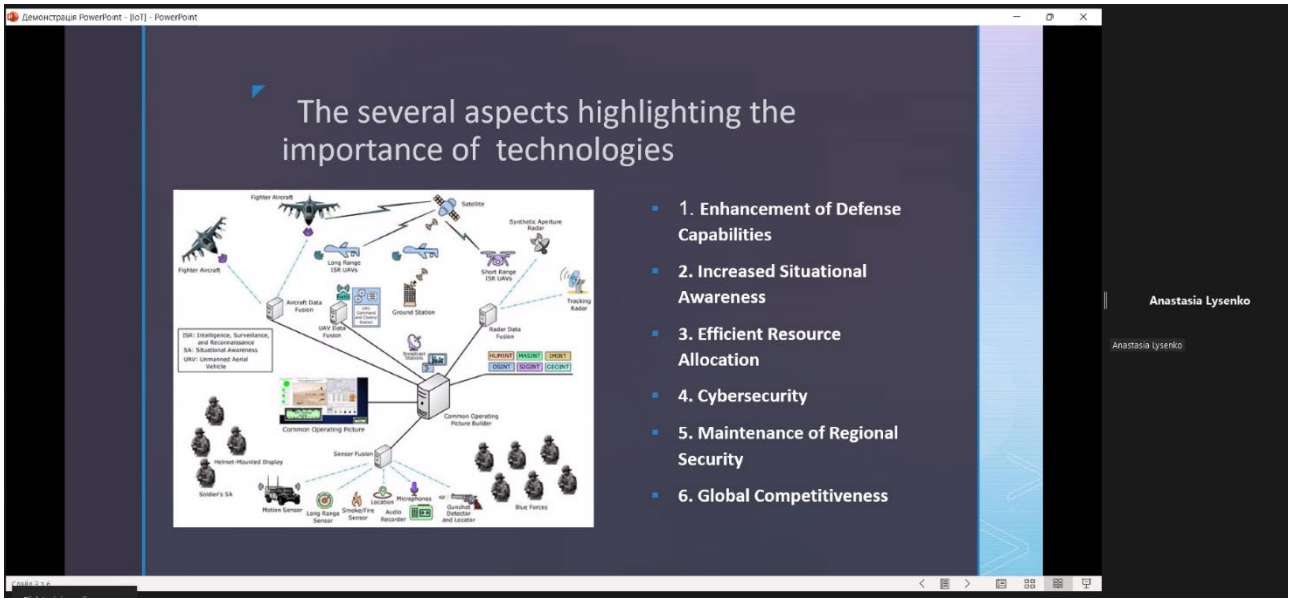
Однак розширення IoT породжує серію викликів у сфері безпеки. По-перше, збільшення обсягу зібраної та обробленої інформації ставить питання конфіденційності даних та несанкціонованого доступу до них. Вдруге, необхідно забезпечити ефективний захист мережі від атак та зловмисних дій у зв'язку з великою кількістю підключених пристроїв. Третє виклик - відсутність стандартів у галузі безпеки, що може призвести до непрозорих взаємодій між різними IoT-продуктами. Четвертий виклик - забезпечення масштабованості заходів безпеки для ефективного захисту великої кількості підключених пристроїв. Нарешті, використання IoT може стати загрозою для приватності та безпеки людей, оскільки багато пристроїв може збирати та передавати особисті дані.

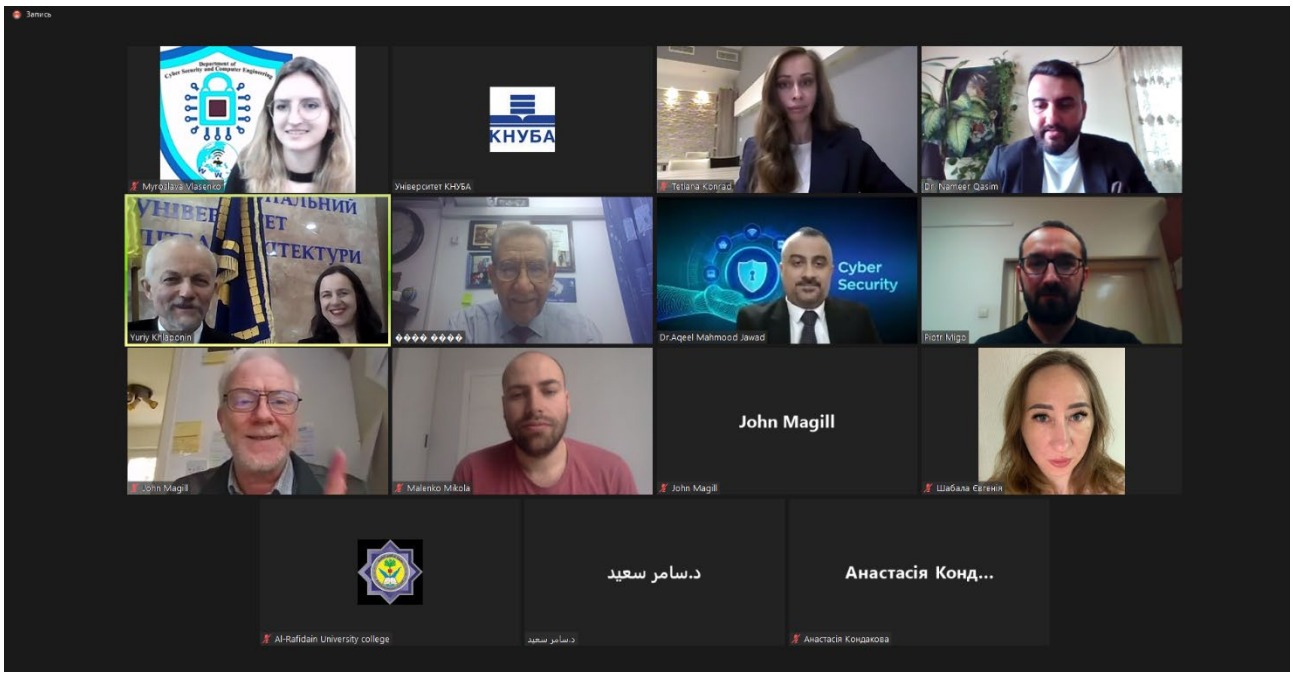
Література

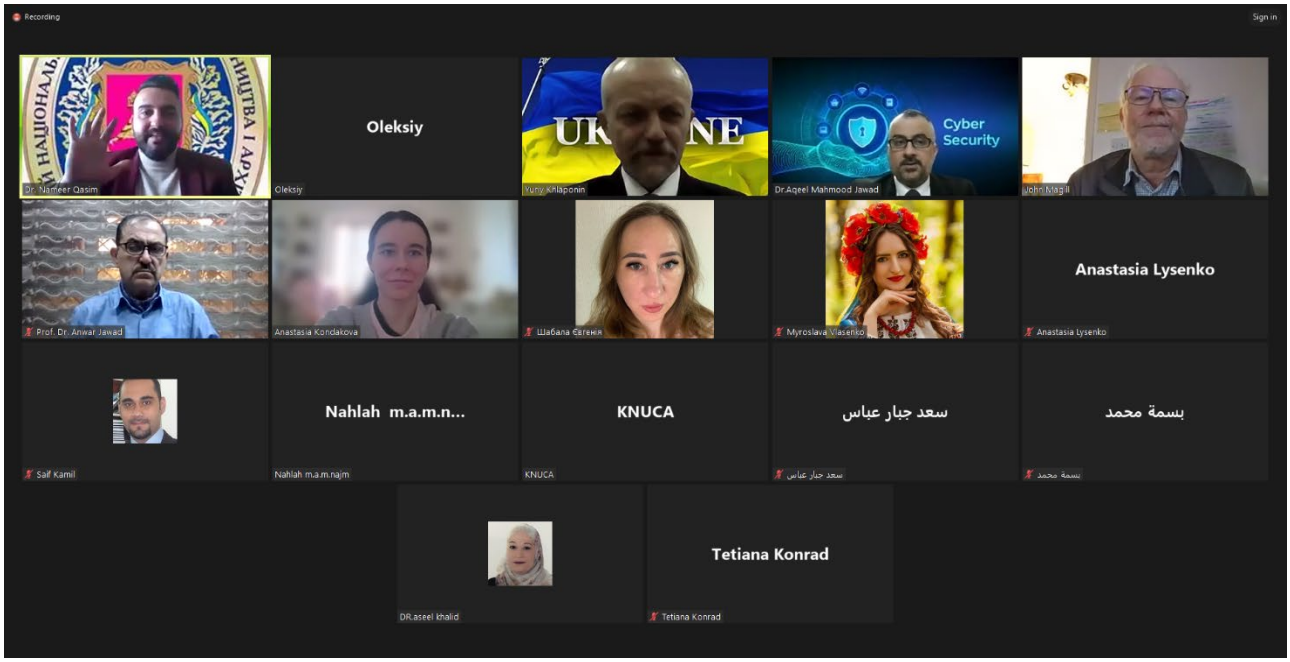
[1] «NIST Special Publication 800-37, Revision 2. Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy, 2018.
[2] Електронне джерело: Безпека IoT-рішень підприємств. Доступ: https://worldvision.com.ua/bezopasnost-iot-resheniy-predpriyatiy/.

ФОТО З КОНФЕРЕНЦІЇ






КНУБА
Cyber Security
John Magill
د.سامر سعيد
Анастасія Конд...


Oleksiy
Cyber Security
Anastasia Lysenko
Nahlah m.a.m.n...
KNUCA
سعد جبار عباس
بسمة محمد
Tetiana Konrad

ДЛЯ НОТАТОК

Наукове видання

III Міжнародна науково-практична конференція “Новітні технологічні тенденції інтелектуальної індустрії та Інтернету речей”

ТЕЗИ ДОПОВІДЕЙ УЧАСНИКІВ
III Міжнародної науково-практичної конференції “Новітні технологічні тенденції інтелектуальної індустрії та Інтернету речей”
25-26 СІЧНЯ 2024 РОКУ

Підписано до друку 05.02.2024. Формат 60x90/16
Ум. друк. арк. 2,5. Обл. вид. 0,9

Видавець і виготовлювач
Київський національний університет будівництва і архітектури
Повітрофлотський проспект, 31. Київ, Україна, 0380