International Journal of Electrical and Computer Engineering (IJECE)
Vol. 15, No. 4, August 2025, pp. 4074∼4086
ISSN: 2088-8708, DOI: 10.11591/ijece.v15i4.pp4074-4086

Assessing the knowledge and practices of internet of things security and privacy among higher education students

Aigul Adamova[1], Tamara Zhukabayeva[1,2], Makpal Zhartybayeva[1,2], Laula Zhumabayeva[3]
[1]Department of Computer Engineering, Astana IT University, Astana, Kazakhstan
[2]Faculty of Information Technology, L.N.Gumilyov Eurasian National University, Astana, Kazakhstan
[3]Department of Computer Science, Yessenov University, Aktau, Kazakhstan

Article Info

Article history:

Received Sep 6, 2024
Revised Apr 2, 2025
Accepted May 24, 2025

Keywords:

Assessing knowledge
Cybersecurity awareness
Higher education students
Internet of things
Network threats
Questionnaire survey

ABSTRACT

When multiple internet of things (IoT) devices interact, there are risks of privacy breaches, personal data leaks, various attacks, and device manipulation. Security is one of the most important technological research problems that currently exist for the IoT. The main purpose of the present paper is to determine the level of awareness of university students about existing security issues when using IoT devices. The paper presented the methodology of the survey. A questionnaire was developed covering four areas, such as fact-finding about general concepts of the IoT, security measures when using IoT devices, security threats and the presence of vulnerabilities of IoT devices, general policies, practices and shared responsibilities. A methodology for calculating the Awareness Level Index is proposed. This study has potential limitations. The effect estimates in the model are based on a survey of undergraduate and master's degree students in "Computer Science" and "Software Engineering" within several universities. A total of 370 undergraduate and master's students participated in the survey. The data processing resulted in the development of recommendations and suggested measures. This study will be useful for both stakeholders and researchers to develop effective strategies and make informed decisions.

Corresponding Author:

Laula Zhumabayeva
Department of Computer Science, Yessenov University
32, Microdistrict, Aktau 130000, Kazakhstan
Email: Laula1.zhumabayeva@yu.edu.kz

1. INTRODUCTION

The development of wireless sensor network technology has led to different categories of internet of things (IoT) devices with respect to the application area, including the consumer IoT, industrial IoT, medical IoT, and others. Different categories of IoT devices in parallel with efficiency and convenience capabilities may lead to new security issues, which in turn may violate privacy [1]–[5]. User awareness of threats and security measures is critical to ensure that IoT devices operate reliably and protect personal data [6], [7]. In a 2023 report, the Netgear security team noted that IoT devices with a high number of vulnerabilities include routers (12%), digital video recorders (13%), smartplugs (18%), and smart TVs (34%) [8]. The intensity of use, duration of operation, and regularity of software updates make devices vulnerable. Researchers highlight the high risk of denial of service attacks (27.20%) and buffer overflow (28.25%) [5], [6]. These vulnerabilities can lead to privilege escalation, memory corruption or overflow, leakage of important information, and in turn, pose significant risks of unauthorized access and system compromise [8]. According to Bitdefender statistics for 2024, approximately 2.5 million threats are blocked every day [9].

Various applications using the IoT create a network of interconnected devices, making it an attractive target for cybercriminals. In 2024, Roku, an American consumer electronics company, experienced a significant increase in cybersecurity threats targeting IoT devices used in smart homes, with over 576,000 accounts compromised. This incident highlights vulnerabilities and underscores the importance of securing devices to protect personal and financial information and maintain the integrity of home networks [10].

Ensuring IoT security is a task that requires collaborative efforts from device manufacturers, service providers, and end users. Only by working together can we create robust protection against cyber threats and ensure a secure future for the IoT. The main goal of this work is to develop an understanding of the safe use of IoT devices. The contributions of this article are as follows: a methodology for raising awareness of IoT device security has been developed; a review and analysis of survey results among students are presented; and recommendations for improving awareness and proper behaviour when working with IoT devices have been formulated.

The rest of the article follows this structure. Section 2 analyzes related work in the research area. Section 3 presents the methodology and content of the survey regarding students' awareness of IoT device security. The survey results and the main conclusions of the study, based on the results obtained, are detailed in section 4. Section 5 presents the conclusion and outlines future work.

2. RELATED WORK

IoT devices continue to be actively integrated into various areas of our lives, and along with this, the need for robust security mechanisms is increasing. Current research on IoT security covers a wide range of areas, including traffic analysis [8], lightweight cryptography [4], machine learning, ensemble learning, and federated learning for anomaly detection [7]–[11]. Importantly, special attention has been given to data privacy, trust management, and protection against unauthorised access [12], [13]. Notably, the diversity of IoT devices such as consumer IoT devices and industrial IoT devices, contributes to unique security challenges [14]. To address security challenges, researchers are developing new methods and algorithms based on analysing device behaviour, detecting anomalies in network traffic, and applying lightweight cryptographic algorithms. In addition, the growth of device-to-device communication in IoT networks emphasises the need for robust security measures to prevent potential attacks and ensure secure data transmission [15]–[17].

Azrour *et al.* [18] in their study presented the results of vulnerability analysis of IoT systems, highlighting common threats such as denial-of-service attacks, data breaches, and privacy violations. The authors propose a number of measures to improve the security of IoT systems, where they emphasise authentication, encryption and access control mechanisms. In parallel, Meylani [19] reported their research results regarding the application of IoT technologies in education. The authors noted that, despite the promising nature of this direction, it is necessary to address a number of problems related to the security and accessibility of such systems, especially in developing countries. Moreover, Wambua [20] presented security challenges regarding the architecture related to the sensor layer, network layer, middleware layer, gateways and application layer. The authors discussed existing and proposed future solutions to IoT security threats via blockchain, fog computing, edge computing and machine learning algorithms. In general, research efforts have focused on enhancing IoT security through innovative approaches, collaborative initiatives, and the development of effective methods using cryptographic solutions to meet the stringent security requirements of modern digital ecosystems [4], [19], [20]. However, these listed aspects of information security emphasise the need to develop robust measures against cyber attacks. In addition, users' awareness of possible cyber threats to the IoT devices they use is important to ensure privacy and further develop the use of IoT devices [19]–[24]. In this context, it is important to pay attention to the level of preparation of the society where IoT devices are actively used.

Numerous studies have identified factors that influence users' awareness of cybersecurity risks [25]–[28]. For example, Pósa and Grossklags [27] presented the results of their research on cybersecurity risk awareness in various categories, two of which are smart home devices and social engineering threats. The authors found that cybersecurity risk awareness is largely associated with university students' experience across a wide range of topics and specific issues. Aljohani and Elfadil [28] proposed a tool to assess the level of cybersecurity awareness among students. The study results indicated an average level of awareness, and the authors provided policy recommendations that should be implemented at their institution. Taha N. and Dahabiyeh L. [29] presented an empirical comparison of cybersecurity awareness among students in terms of knowledge and behaviour. The study revealed that students are well informed about some cybersecurity concepts. In [30], a systematic review was conducted to examine the current literature on the role of individuals in strengthening cybersecurity defences. The authors highlighted several open questions regarding the development of training programs, awareness-raising campaigns, and information sharing about the nature and types of cyberattacks.

The security of IoT devices is a multidimensional problem that requires a comprehensive approach. As a result of the analysis of current research, Figure 1 presents a taxonomy of IoT security issues. One of the key factors determining the security level of IoT systems is the human factor. Empirical studies have shown that users' awareness of cyber threats is directly related to their behaviour in the digital environment. In this context, one of the urgent tasks is to develop effective training programs aimed at increasing the level of cyber literacy of users. The present study reveals a number of open questions that require further research.

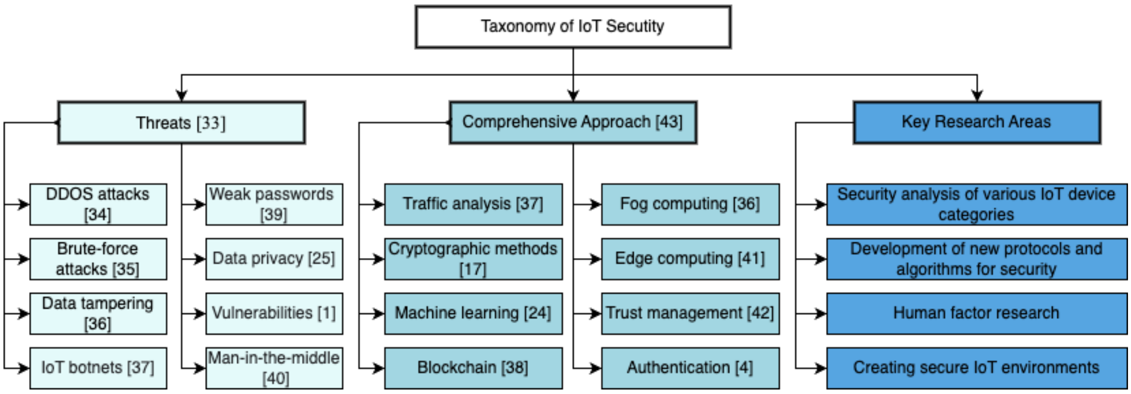


Figure 1. Taxonomy of IoT security

The presented taxonomy structures the field of IoT security research around three main branches, such as threat types, multidimensional approaches, and key research directions. The analysis of studies [1], [21], [29]–[35] allowed us to systematise the spectrum of the most significant threats specific to IoT devices. The comprehensive approach presents various methods and technologies that can be used to ensure security [4], [15], [20], [32], [33], [36]–[42]. The key directions of the research area are as follows: analysing the security of different categories of IoT devices; developing new protocols and cryptographic algorithms; and, along with this, studying the impact of human factors. Research on human factors involves analysing the impact of human behaviour on the security of IoT systems. The presented taxonomy emphasises that securing IoT systems requires a comprehensive approach that includes both technical and organisational measures.

3. MATERIALS AND METHODS

This section presents the methodology and content of the survey. We present a formula for calculating the index to obtain a general indicator of respondents' awareness levels. The proposed classification of the index of awareness levels helps reduce the obtained information to a single quantitative value for further analysis.

At the initial stages, a conceptual framework for the study was created, where the main variables and indicators were defined; then, questions with answer options were compiled and categorised. Empirical data were collected as part of a study at one university during the academic year 2023-2024. The survey involved undergraduate and graduate students in Computer Science and Software Engineering programs. Before the questionnaire was sent to the respondents, all the questions were checked by experts. After completing the peer review and pilot study, the questionnaire was sent to the respondents via e-mail wia the MS Outlook service. Typically, the survey approach involves a two-stage process, as shown in Figure 2. The first stage involves the respondents, whereas the second stage analyses the answers received from the respondents. Each stage consists of certain tasks. The survey was voluntary, and everyone was welcome to participate. Furthermore, all the responses received were checked and analysed. At the final stage of the research, recommendations were developed.

In the present study, we divided the methodology into two stages: survey and data mining. We divided the questionnaire into four areas: general concepts, common security issues, existing risks and vulnerabilities, and liability policies for the use of IoT devices. To ensure a clear and accurate understanding of each issue, we developed a set of clarifying questions, which are displayed in Table 1. The survey used a standardised set of questions with predefined alternative answers, which simplified the data analysis. We also used an online survey to cover a large audience and reduce the time required for data collection.

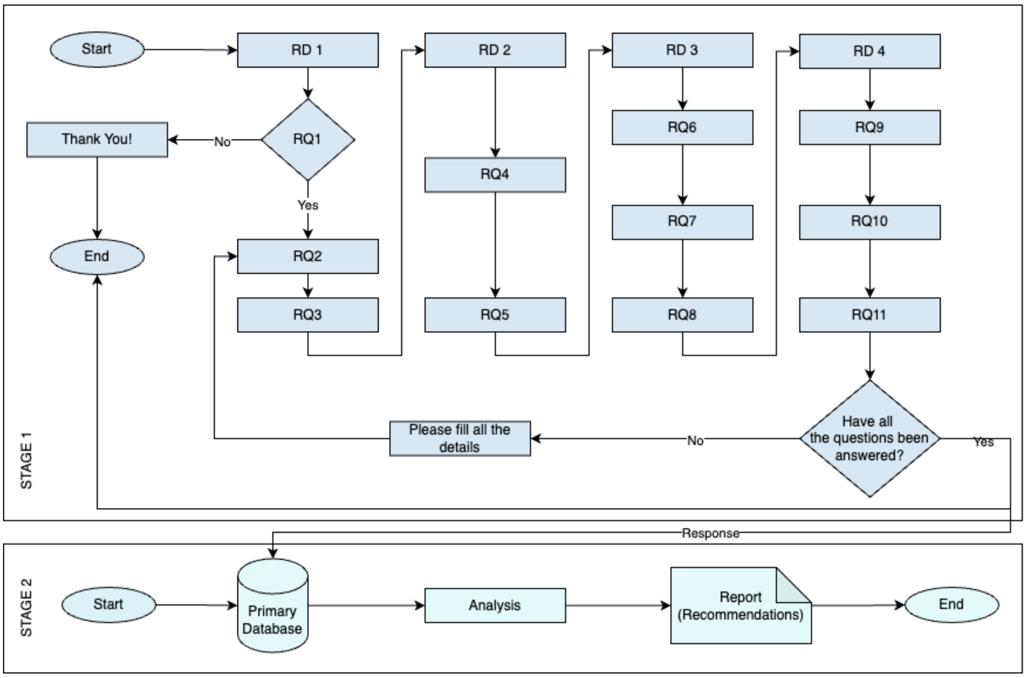


Figure 2. Survey methodology

Table 1. Research direction/research question

Research direction	Research question
RD1. Understanding IoT devices	RQ1. Are you aware of what the term IoT refers to and what it means?
	RQ2. What do you think are the main functions of IoT devices?
	RQ3. Which IoT platforms have you had experience with?
RD2. Security issues with IoT devices	RQ4. How worried are you that someone might access your personal data through smart devices?
	RQ5. Which organizations, in your opinion, should be responsible for IoT device security?
RD3. Security threats and vulnerabilities of IoT devices	RQ6. Are you familiar with the vulnerabilities of IoT devices?
	RQ7. What IoT security issues have you encountered or heard about?
	RQ8. What are the most critical security threats?
RD4. Practices and general responsibility	RQ9. The importance of built-in security features?
	RQ10. Security measures adopted by participants?
	RQ11. What do you think are the most effective ways to improve the security of IoT devices?

The respondents were undergraduate and graduate students from various universities. We informed the purpose of the research and guaranteed anonymity of personal data to a total of 370 respondents who participated in the survey. Participation in the survey was entirely voluntary. Response duration averaged between 7 and 10 minutes. Figure 3 shows the dashboard with the input of research data. The information is presented by level of study (undergraduate, graduate), participants by gender, percentage of respondents' participation by universities, possible indicators of awareness, and type of survey.

To obtain an overall measure of respondents' awareness, we propose the use of the Awareness Level Index (ALI). In this study, the ALI index is used to provide further recommendations. In our research, ALI is calculated on the basis of responses to questions RQ3, RQ4, RQ5, RQ9, and RQ11. The ALI calculation is performed via formula (1):

$$ALI = \frac{SUM(RQ\ weight * User\ answer) * 100)}{Maximum\ possible\ score\ of\ RQ3, RQ5,\ RQ9,\ RQ11} \quad (1)$$

where RQ weight, the weight of a question, reflects its significance for the overall assessment of the awareness level. For example, questions about understanding basic terms may carry less weight than questions about practical skills do.

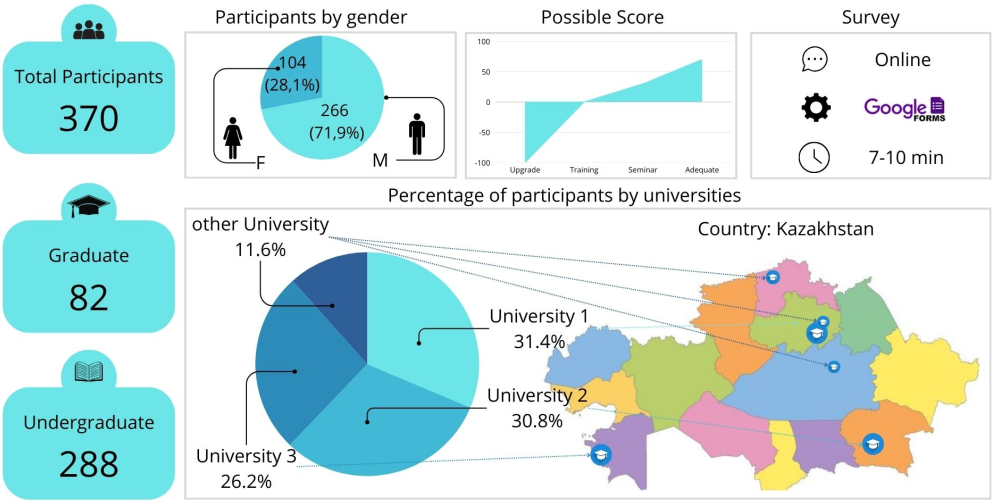


Figure 3. Survey dashboard

User answer - score assigned to each user's response. In our survey, the scale is divided by quality, e.g., in RQ9, response options are ”slightly important,” ”important,” and ”very important”. Maximum possible score - Maximum value, the highest score the index can achieve if the user answers all questions correctly. The calculated ALI was classified into the following ranges:

– (-100-0): Requires an increase in awareness level;
– (0–30): Requires attending training on secure IoT device configuration;
– (30–70): Requires a seminar on analysing the most common threats to IoT systems;
– (70–100): Adequate level of awareness.

These ranges help to consolidate the overall understanding of users into a single quantitative value and analyse the results.

4. DATA ANALYSIS AND RESULTS

This section presents the results of the survey. The results for each question are shown both as percentages and in absolute numbers. 370 undergraduate and graduate students expressed a desire to take part in the survey, but according to the results of the first question, the number of respondents was 351.

For the RD1 direction, two questions were included. Overall, for RQ1, the majority of the respondents demonstrated familiarity with the concept of the IoT. 19 respondents indicated that they were not familiar with it at all, whereas 101 respondents noted that they were somewhat familiar with the concept of the IoT. The majority of the participants, 37.8% (140 respondents), stated that they were moderately familiar, and 29.7% (110 respondents) claimed to be well acquainted with the term ”Internet of Things” and understood its meaning. The analysis of the survey results revealed that the respondents generally demonstrated a sufficient level of understanding of the IoT concept, which is important to form an adequate assessment of the relevant security issues. 5.1% (19 participants) indicated that they were not familiar with the IoT concept; as a result, they were thanked for their participation, and their responses were excluded from the analysis of subsequent questions. The percentage distribution of responses to RQ1 is shown in Figure 4. Thus, the second and subsequent survey questions are based on the answers of the 351 participants.

RQ2 aims to provide a comprehensive view of respondents' perceptions of IoT device functionalities. The respondents were given options, including general functions such as data collection, device management, process automation, and security. Multiple categories can be selected. The results are displayed in Figure 5. All the respondents selected data collection as a function, 98.3% chose security, 80.91% noted process automation, and 64.1% selected device management.

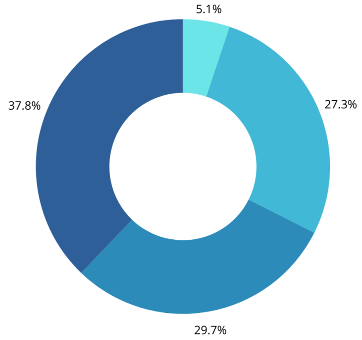


Figure 4. Percentage of participants for RQ1

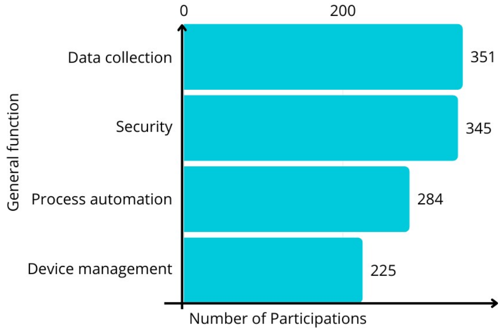


Figure 5. Percentage of participants for RQ2

RQ3 provides the most comprehensive information about which IoT platforms respondents are familiar with and their level of experience. This allows us to assess the popularity of different platforms, identify knowledge gaps and plan further recommendations. Analysing the results, we can note the three most popular platforms among respondents: Microsoft Azure IoT Hub, Amazon Web Services IoT Core, and Google Cloud IoT Core, for which there are even experts. The respondents are not at all familiar with the IBM Watson IoT Platform, Salesforce IoT Cloud, or Kaa IoT Platform. The ThingWorx IoT Platform, Artik Samsung Electronics, Cisco IoT Cloud Connect, and ThingSpeak were selected by the respondents as 1-2 times of use, and some respondents noted that they were not familiar with them. The quantitative indicators by platform are shown in Figure 6.

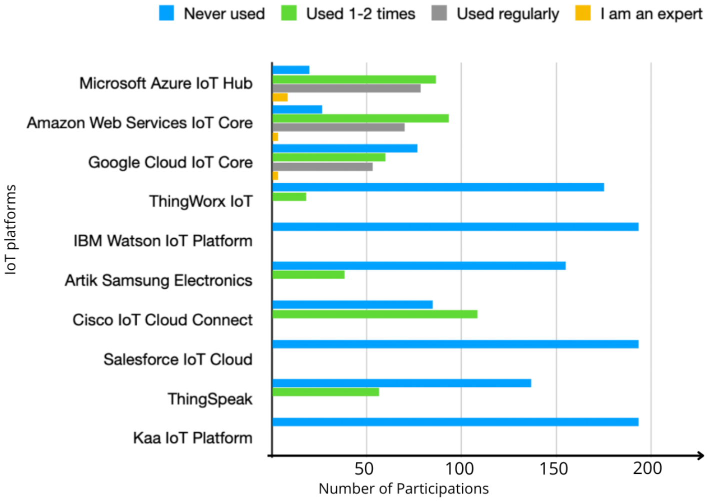


Figure 6. Quantitative indicators of respondents' answers to RQ3

RD2 explores security issues in the use of IoT devices. The data from questions RQ4 and RQ5 provide insight into respondents' understanding of basic security measures for IoT devices. Two questions were formulated: RQ4 identifies how concerned respondents are about the security of IoT devices. RQ5 is an open-ended question to identify perceptions of responsibility allocation. The results of the survey for RQ4 are shown in Figure 7, where 51.8% of the respondents showed serious concern, 32.1% of the respondents had a medium level of concern and 16.1% showed a slight level of concern. For RQ5, there was a question about the need to share responsibility between users, manufacturers and suppliers, which was answered with “yes” by 48.21%, “no” by 15.18% and “depends” by 36.61%, as shown in Figure 8.

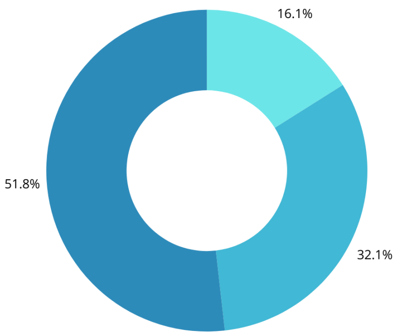


Figure 7. Percentage of participants for RQ4

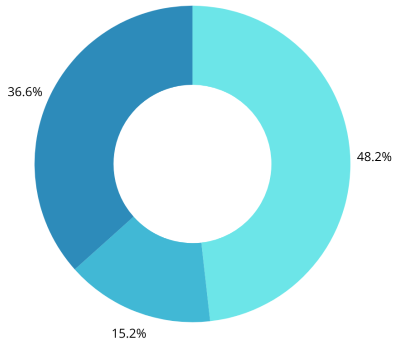


Figure 8. Percentage of participants for RQ5

RD3 determines the level of participants’ awareness of common IoT security vulnerabilities, their familiarity with IoT security threats and their perception of the most important security threats. There are 3 questions to be answered for this strand. RQ6 establishes the level of familiarity with the common security vulnerabilities of IoT devices. RQ7 establishes the level of familiarity with the possible threats posed by IoT devices. RQ7 prioritizes the most important security threats.

For RQ6, we asked about their awareness of common IoT security vulnerabilities, and the majority (63.2%, 222 respondents) identified weak or easily guessed passwords as vulnerabilities. Lack of regular security updates and patches was the second most popular issue (47.29%, 166 respondents), followed by insecure remote control access, lack of encryption in data transmission, and access to equipment by users with limited knowledge, each with 36.75% (out of 129 respondents) admitting to it. In addition, 110 respondents (31.34%) mentioned the vulnerability of inadequate user authentication and authorization. The results are summarized in Figure 9.

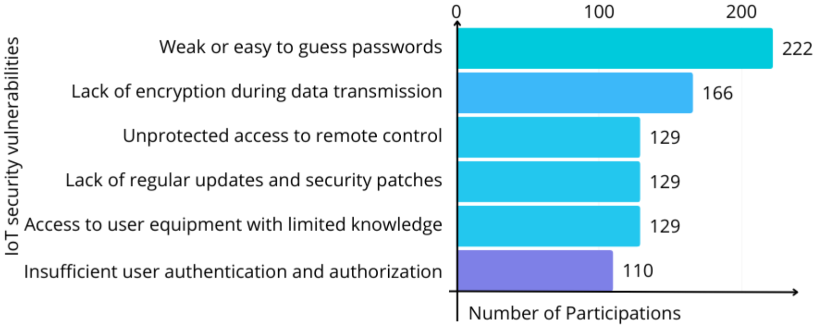


Figure 9. Percentage of participants for RQ6

RQ7 identifies the most familiar IoT security threats to respondents. Figure 10 shows the results; according to the findings, the most popular threat was unauthorized access; 66.3% of the respondents (233 respondents) were familiar with it. DDoS attacks were familiar to 63.9% of the participants (224 respondents), and 31.2% (110 respondents) were familiar with physical attacks. A total of 27.3% (out of 96 respondents) said they were familiar with spoofing, and 24.9% (87 respondents) chose MITM attacks. Only 17.01% (60 respondents) chose the Sinkhole attack option.

Question RQ8 helps identify the most significant security threat from the respondents’ perspective. Among the threats listed, unauthorised access was the greatest concern for 38.9% of the respondents

(144 respondents). DDoS attacks were closely followed by 27.3% of the respondents (101 respondents), who considered them the most serious threat. Spoofing attacks were considered the most important attack by 10,5% (39 respondents), whereas Malware attacks were chosen by 10,3% (38 respondents). Only 29 respondents (8%) considered MITM attacs to be the least important. The results are displayed in Figure 11.

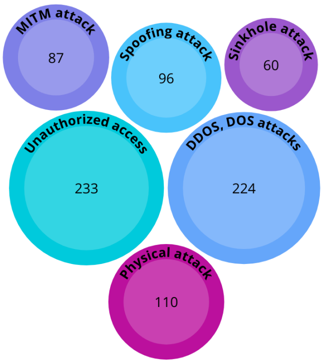


Figure 10. Percentage of participants for RQ7

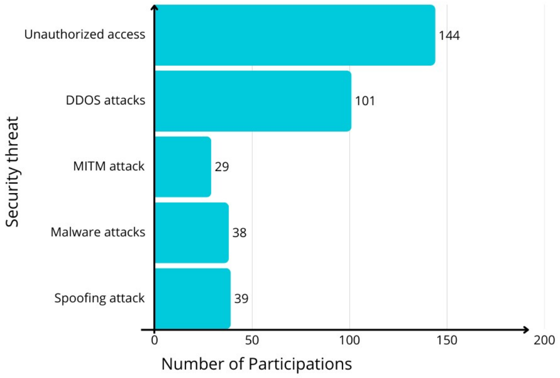


Figure 11. Percentage of participants for RQ8

Survey strand RD4 examines the importance of built-in security features in IoT devices, the security measures they take to protect their devices, the importance of user education, and the most effective protection methods for improving the security of IoT devices. Question RQ9 investigated how important built-in security features are to respondents. As a result, 99 respondents (28.3%) indicated “very important”, with the “important” selected by 168 respondents (47,8%) and “somewhat important” categories selected by 84 respondents (23.9%), as shown in Figure 12.

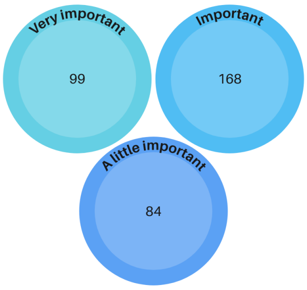


Figure 12. Importance of the built-in functions of the RQ9

Question RQ10 also seeks to understand what measures participants take to protect their IoT devices. The most common security measure was changing default passwords, a practice implemented by 56.12% (197 respondents). The second most popular measure was using different encryption methods for data transfer by 41.6% (146 respondents). The third place measure was monitoring network traffic for unusual data by 40.5% (142 respondents). The regularly updating device firmware and remote device management were mentioned by 39.6% (139 respondents), and using devices with Secure Shell (SSH) security measures, with a share of 29.3% (103 respondents). A total of 16.5% (58 respondents) mentioned using IoXT-certified devices. The results are shown in Figure 13.

When asked by RQ11 about the most effective way to improve the security of IoT devices, 41.96% (147 respondents) chose increased device security from manufacturers, followed by increased user awareness and education (34.82%, 122 respondents), security technology development (16.96%, 56 respondents), and stricter regulations (3.57%, 13 respondents). Nine respondents (2.68%) mentioned open source hardware as a possible solution. The analysis of the results reveals different opinions on the most effective ways to improve the security of IoT devices, with an emphasis on the role of manufacturers and user awareness. The percentage of participants is shown in Figure 14.

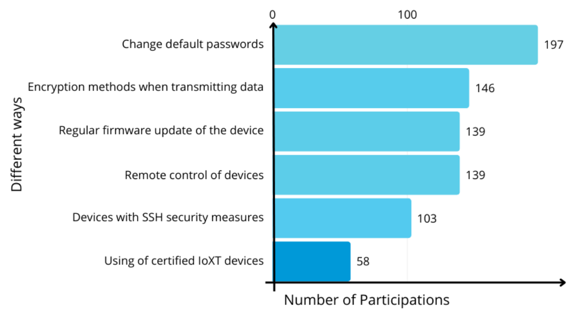


Figure 13. Percentage of participants for RQ10

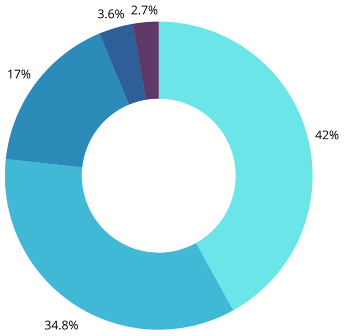


Figure 14. Percentage of participants for RQ11

The present study compared learners' awareness of IoT technologies, possible threats and vulnerabilities in the use of IoT devices, policies and general responsibilities. The preliminary assessment demonstrated that not all learners have a sufficient understanding, in general, of both IoT technologies and existing threats and vulnerabilities. The survey was exploratory in nature, and participation was voluntary. Data were collected from the learners where the issues of data security, integrity and confidentiality were covered in different areas of learning. The questions that were designed assume that the respondents have experience using IoT devices. In the survey, 5.1% of the respondents said they were not familiar with the concept of the IoT, and 27.3% said they were somewhat familiar. These are relatively small numbers, but owing to the widespread adoption of IoT technologies in everyday life, learners and users in general need to be aware of them and the implications of their use. The need to increase the basic knowledge of users with a focus on security can also be noted. In particular, training on the secure configuration of IoT devices, selection of strong passwords, and software updates should be covered. Conducting training and workshops to analyse the most common threats to IoT systems, such as DDoS attacks, device hacking, and data breaches, can also increase the awareness levels noted in Figure 15. In addition to further validation of this tool with other respondents, more research is needed on the intention to utilise security best practices with respect to the IoT.

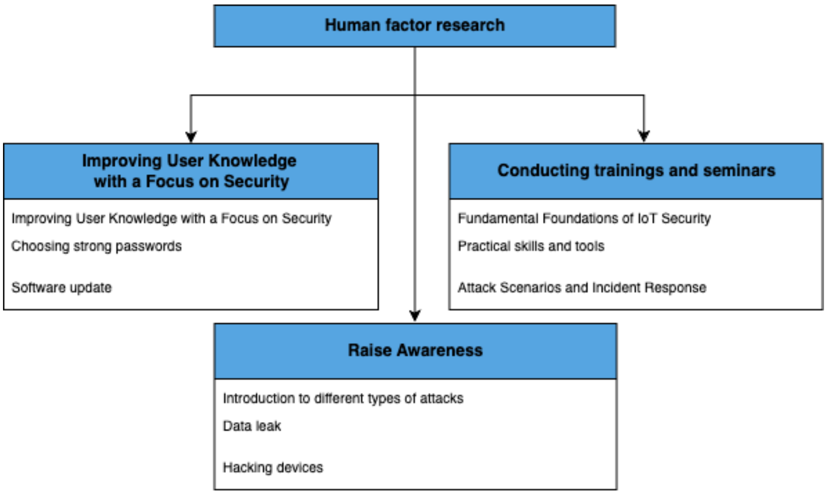

Human factor research
Improving User Knowledge with a Focus on Security
Improving User Knowledge with a Focus on Security
Choosing strong passwords
Software update
Conducting trainings and seminars
Fundamental Foundations of IoT Security
Practical skills and tools
Attack Scenarios and Incident Response
Raise Awareness
Introduction to different types of attacks
Data leak
Hacking devices

Figure 15. Directions of research

The research question concerning the awareness level of university students about existing security issues when IoT devices are used is displayed in three main areas: raising user awareness, conducting training and seminars and raising general awareness. The results of our study indicate the need for further research to develop effective methodologies to assess the level of cybersecurity of IoT device users. This will allow for a more accurate assessment of the effectiveness of educational programs and the development of targeted awareness-raising measures.

5. CONCLUSION

The study was conducted to develop an understanding of the safe use of IoT technologies. The presented research methodology for IoT device safety awareness assessment allows the level and directions for future research to be determined. Moreover, we propose to use an awareness level index. The parsing and analysis of the learner survey results demonstrated an average level of awareness, which demonstrates the need for various integrated methods to increase awareness and develop skills for the safe use of IoT devices.

The results of the study show that the level of user awareness of the safe use of IoT technologies remains at an average level, which is generally consistent with the data of previous studies. It is important to note that, unlike the aforementioned works, the current study demonstrates a high level of knowledge among university students, which is directly related to the increased availability of educational materials and the relevance of cybersecurity issues. An important thing about this study is that it used both quantitative and qualitative methods to collect data, which let the researchers get a better understanding of how users behave.

As a weakness, it is worth noting the relatively small sample (N = 370), which may reduce the possibility of generalizing the results to a wider audience. It was unexpected to identify the proportion of users (more than 10%) who are not familiar with the concept of the Internet of Things. This indicates that, despite the active distribution of IoT devices in everyday life, a significant portion of people are not aware of their presence or do not associate them with the general concept of IoT. This may be because many devices, such as smart speakers, smart home systems, and wearables, are perceived by users as standalone technologies rather than as part of a unified ecosystem. This finding highlights the need for more active information education about the Internet of Things and its security risks. A lack of basic knowledge can lead to misuse of such devices, increasing the likelihood of cyberattacks, data leaks, and other threats. Further research can be aimed at studying the influence of various factors on the level of cyber literacy of IoT users, as well as at developing new methodologies for assessing the effectiveness of educational programs in the field of cybersecurity. In addition, an interesting direction for future research is to study the relationship between the level of cyber literacy of users and their online behaviour.

ACKNOWLEDGEMENTS

This work was supported by Astana IT University.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Aigul Adamova	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓	
Tamara Zhukabayeva	✓	✓				✓		✓	✓	✓	✓	✓		
Makpal Zhartybayeva	✓		✓	✓		✓	✓		✓		✓		✓	
Laula Zhumabayeva					✓		✓			✓		✓		✓

C	: Conceptualization
M	: Methodology
So	: Software
Va	: Validation
Fo	: Formal Analysis
I	: Investigation
R	: Resources
D	: Data Curation
O	: Writing - Original Draft
E	: Writing - Review & Editing
Vi	: Visualization
Su	: Supervision
P	: Project Administration
Fu	: Funding Acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data, which contain information that could compromise the privacy of research participants, are not publicly available due to certain restrictions.

REFERENCES

[1] S. A. Baho and J. Abawajy, “Analysis of consumer IoT device vulnerability quantification frameworks,” *Electronics*, vol. 12, no. 5, p. 1176, Feb. 2023, doi: 10.3390/electronics12051176.

[2] R. Kumar and N. Agrawal, “Analysis of multi-dimensional industrial IoT (IIoT) data in edge–fog–cloud based architectural frameworks: A survey on current state and research challenges,” *Journal of Industrial Information Integration*, vol. 35, p. 100504, Oct. 2023, doi: 10.1016/j.jii.2023.100504.

[3] F. Subhan *et al.*, “AI-enabled wearable medical internet of things in healthcare system: A survey,” *Applied Sciences*, vol. 13, no. 3, p. 1394, Jan. 2023, doi: 10.3390/app13031394.

[4] M. Z. Khan, K. U. Nisa, M. T. Quasim, M. A. Khalifa, and M. M. Mobarak, “Cloud-based data protection: A framework for authorizing data movement,” *2024 International Conference on Expert Clouds and Applications (ICOECA)*, pp. 271–275, Apr. 2024, doi: 10.1109/icoeca62351.2024.00057.

[5] J. M. Fernández-Batanero, M. Montenegro-Rueda, J. Fernández-Cerero, and E. López Menéses, “Adoption of the internet of things in higher education: Opportunities and challenges,” *Interactive Technology and Smart Education*, vol. 21, no. 2, pp. 292–307, Aug. 2023, doi: 10.1108/itse-01-2023-0025.

[6] B. Tabuenca, J.-L. Moreno-Sancho, J. Arquero-Gallego, W. Greller, and D. Hernández-Leo, “Generating an environmental awareness system for learning using IoT technology,” *Internet of Things*, vol. 22, p. 100756, Jul. 2023, doi: 10.1016/j.iot.2023.100756.

[7] IDC, “Future of industry ecosystems: Shared data and insights,” *IDC*, 2022. https://blogs.idc.com/ (accessed on Aug. 21, 2024).

[8] Netgear, “2024 IoT threat report, *Netgear*, 2024. https://www.netgear.com/hub/network/2024-iot-threat-report/ (accessed on Aug. 20, 2024).

[9] “2024 IoT security landscape report,” *Bitdefender*, [Online]. Available: https://blogapp.bitdefender.com/ (accessed on Aug. 26, 2024).

[10] G. Vadivel, M. J. M. Hussain, S. V. Tresa, and S., “Smart transportation systems: IoT-connected wireless sensor networks for traffic congestion management,” *International Journal of Advances in Signal and Image Sciences*, vol. 9, no. 1, pp. 40–49, Jun. 2023, doi: 10.29284/ijasis.9.1.2023.40-49.

[11] A. Adamova, T. Zhukabayeva, and Y. Mardenov, “Machine learning in action: An analysis of its application for fault detection in wireless sensor networks,” *2023 IEEE International Conference on Smart Information Systems and Technologies (SIST)*, May 2023, doi: 10.1109/sist58284.2023.10223548.

[12] Y. Alotaibi and M. Ilyas, “Ensemble-learning framework for intrusion detection to enhance internet of things’ devices security,” *Sensors*, vol. 23, no. 12, p. 5568, Jun. 2023, doi: 10.3390/s23125568.

[13] R. Lazzarini, H. Tianfield, and V. Charissis, “Federated learning for IoT intrusion detection,” *AI*, vol. 4, no. 3, pp. 509–530, Jul. 2023, doi: 10.3390/ai4030028.

[14] P. M. Rao and B. D. Deebak, “A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions,” *Ad Hoc Networks*, vol. 146, p. 103159, Jul. 2023, doi: 10.1016/j.adhoc.2023.103159.

[15] A. E. Omolara *et al.*, “The internet of things security: A survey encompassing unexplored areas and new insights,” *Computers & Security*, vol. 112, p. 102494, Jan. 2022, doi: 10.1016/j.cose.2021.102494.

[16] M. Douiba, S. Benkirane, A. Guezzaz, and M. Azrour, “An improved anomaly detection model for iot security using decision tree and gradient boosting,” *The Journal of Supercomputing*, vol. 79, no. 3, pp. 3392–3411, Sep. 2022, doi: 10.1007/s11227-022-04783-y.

[17] F. Thabit, O. Can, A. O. Aljahdali, G. H. Al-Gaphari, and H. A. Alkhzaimi, “Cryptography algorithms for enhancing internet of things security,” *Internet of Things*, vol. 22, p. 100759, Jul. 2023, doi: 10.1016/j.iot.2023.100759.

[18] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, “Internet of things security: Challenges and key issues,” *Security and Communication Networks*, vol. 2021, pp. 1–11, Sep. 2021, doi: 10.1155/2021/5533843.

[19] R. Meylani, “Transforming education with the internet of things: A journey into smarter learning environments,” *International Journal of Research in Education and Science*, vol. 10, no. 1, pp. 161–178, Feb. 2024, doi: 10.46328/ijres.3362.

[20] R. N. Wambua, “Internet of things security and privacy in higher education institutions in developing countries,” *Research Journal of Education, Teaching and Curriculum Studies*, vol. 2, no. 1, pp. 1–7, Mar. 2024, doi: 10.58721/rjetcs.v2i1.463.

[21] M. S. Mahmood and N. B. Al Dabagh, “Improving iot security using lightweight based deep learning protection model,” *Tikrit Journal of Engineering Sciences*, vol. 30, no. 1, pp. 119–129, Mar. 2023, doi: 10.25130/tjes.30.1.12.

[22] I. Zakariyya, H. Kalutarage, and M. O. Al-Kadri, “Towards a robust, effective and resource efficient machine learning technique for iot security monitoring,” *Computers & Security*, vol. 133, p. 103388, Oct. 2023, doi: 10.1016/j.cose.2023.103388.

[23] K. Y. Najmi, M. A. AlZain, M. Masud, N. Z. Jhanjhi, J. Al-Amri, and M. Baz, “A survey on security threats and countermeasures in iot to achieve users confidentiality and reliability,” *Materials Today: Proceedings*, vol. 81, pp. 377–382, 2023, doi: 10.1016/j.matpr.2021.03.417.

[24] M. A. Azad, S. Abdullah, J. Arshad, H. Lallie, and Y. H. Ahmed, “Verify and trust: A multidimensional survey of zero-trust security in the age of internet of things,” *Internet of Things*, vol. 27, p. 101227, Oct. 2024, doi: 10.1016/j.iot.2024.101227.

[25] B. Cremonezi, A. B. Vieira, J. Nacif, E. F. Silva, and M. Nogueira, "Identity management for internet of things: Concepts, challenges and opportunities," *Computer Communications*, vol. 224, pp. 72–94, Aug. 2024, doi: 10.1016/j.comcom.2024.05.014.

[26] H. Du *et al.*, "Rethinking wireless communication security in semantic internet of things," *IEEE Wireless Communications*, vol. 30, no. 3, pp. 36–43, Jun. 2023, doi: 10.1109/mwc.011.2200547.

[27] T. Pósa and J. Grossklags, "Work experience as a factor in cyber-security risk awareness: A survey study with university students," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 490–515, Jun. 2022, doi: 10.3390/jcp2030025.

[28] W. Aljohni, N. Elfadil, M. Jarajreh, and M. Gasmelsied, "Cybersecurity awareness level: The case of Saudi Arabia university students," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 3, 2021, doi: 10.14569/ijacsa.2021.0120334.

[29] N. Taha and L. Dahabiyeh, "College students information security awareness: A comparison between smartphones and computers," *Education and Information Technologies*, vol. 26, no. 2, pp. 1721–1736, Sep. 2020, doi: 10.1007/s10639-020-10330-0.

[30] S. Nifakos *et al.*, "Influence of human factors on cyber security within healthcare organisations: A systematic review," *Sensors*, vol. 21, no. 15, p. 5119, Jul. 2021, doi: 10.3390/s21155119.

[31] P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, "A survey on security in internet of things with a focus on the impact of emerging technologies," *Internet of Things*, vol. 19, p. 100564, Aug. 2022, doi: 10.1016/j.iot.2022.100564.

[32] D. M. Rajan and S. Sathya Priya, "DDoS mitigation techniques in iot: A survey," *2022 International Conference on IoT and Blockchain Technology (ICIBT)*, pp. 1–7, May 2022, doi: 10.1109/icibt52874.2022.9807799.

[33] C. Faircloth, G. Hartzell, N. Callahan, and S. Bhunia, "A study on brute force attack on T-Mobile leading to sim-hijacking and identity-theft," *2022 IEEE World AI IoT Congress (AIIoT)*, Jun. 2022, doi: 10.1109/aiiot54504.2022.9817175.

[34] S. I. Popoola, B. Adebisi, M. Hammoudeh, G. Gui, and H. Gacanin, "Hybrid deep learning for botnet attack detection in the internet-of-things networks," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4944–4956, Mar. 2021, doi: 10.1109/jiot.2020.3034156.

[35] N. Alsharari, "Integrating blockchain technology with internet of things to efficiency," *International Journal of Technology, Innovation and Management (IJTIM)*, vol. 1, no. 2, pp. 01–13, Dec. 2021, doi: 10.54489/ijtim.v1i2.25.

[36] N. Haider and C. Azad, "Data security and privacy in fog computing applications," *Cloud and Fog Computing Platforms for Internet of Things*, pp. 57–66, Apr. 2022, doi: 10.1201/9781003213888-5.

[37] Y. Lu, "Security and privacy of internet of things: A review of challenges and solutions," *Journal of Cyber Security and Mobility*, Nov. 2023, doi: 10.13052/jcsm2245-1439.1261.

[38] P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, "Internet of things: Security and solutions survey," *Sensors*, vol. 22, no. 19, p. 7433, Sep. 2022, doi: 10.3390/s22197433.

[39] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A survey on security and privacy issues in edge-computing-assisted internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4004–4022, Mar. 2021, doi: 10.1109/jiot.2020.3015432.

[40] A. Sharma, E. S. Pilli, A. P. Mazumdar, and P. Gera, "Towards trustworthy internet of things: A survey on trust management applications and schemes," *Computer Communications*, vol. 160, pp. 475–493, Jul. 2020, doi: 10.1016/j.comcom.2020.06.030.

[41] N. B. Halima, A. S. Alluhaidan, M. Z. Khan, M. S. Husain, and M. A. Khan, "A service-categorized security scheme with physical unclonable functions for internet of vehicles," *Journal of Big Data*, vol. 10, no. 1, p. 178, 2023.

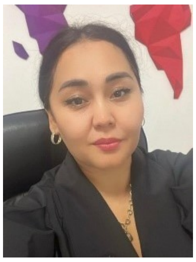
[42] M. S. Husain and M. Z. Khan, Eds., *Critical Concepts, Standards, and Techniques in Cyber Forensics*. IGI Global, 2020. doi: 10.4018/978-1-7998-1558-7.

BIOGRAPHIES OF AUTHORS

Aigul Adamova is an assistant professor at the Department of Computer Engineering, Astana IT University, Kazakhstan. She holds a Ph.D. degree in computing and software. She is an assistant professor of the Department of Computer Engineering, Astana IT University. She has about 40 published papers in refereed journals and conferences. She served as a reviewer for international conferences, including IEEE: SIST 2023, SIST 2024. Her research areas are information security of internet of things, wireless sensor network, embedded system, cyberphysical system, and computer vision. She can be contacted at email: aigul.adamova@astanait.edu.kz.

Tamara Zhukabayeva received the Ph.D. degree from Satbayev University, Kazakhstan. She is currently an associate professor in informatics, computer engineering, and management with L. N. Gumilyov Eurasian National University, Astana, Kazakhstan. She is also an associate member of the Universal Association of Computer and Electronics Engineers, and has membership in scientific societies in the Society of Digital Information and Wireless Communications (SDIWC) and the Universal Association of Computer and Electronics Engineers. She has published over 70 scientific and educational-methodical works: in the Republic of Kazakhstan, and in countries of far and near abroad, including a foreign edition from the Clarivate Analytics Database, Scopus. She is the author and coauthor of educational publications and scientific monographs, and has an innovative patent and copyright certificates for intellectual property rights. She can be contacted at email: tamara.kokenovna@gmail.com.

Makpal Zhartybayeva received the B.S. and M.S. degrees in applied computer engineering and software from Satbayev Kazakh National Technical University in 2012, and the Ph.D. degree in the same specialty from the Gumilyov Eurasian National University in 2020. She is the author of three books and more than 20 articles. She is an associate professor of the Department of Computer and Software Engineering, L. N. Gumilyov ENU, head of the research project, holder of a state scholarship for young and talented scientists of the Republic of Kazakhstan (2018), with experience in the direction of the project for nine years. Her scientific interests include green technologies, development of mobile robotic systems, georadar research, development of an information system for optimizing monitoring of environmental pollution, and wireless sensor network. She can be contacted at email: Makkenskii@mail.ru.



Laula Zhumabayeva is an associate professor in the Department of Computer Science, Yessenov University, Kazakhstan. She holds a Ph.D. in computer science and software engineering. She has about 15 published papers in peer-reviewed journals and conferences. Her research areas include computer simulation, artificial intelligence, parallel computing, and wireless sensor network. She can be reached via email at: laula1.zhumabayeva@yu.edu.kz.