REPUBLIC OF AZERBAIJAN

On the right of the manuscript

ABSTRACT

of the dissertation for the degree of Doctor of Philosophy

DEVELOPMENT OF METHODS AND ALGORITHMS FOR ENSURING INFORMATION SECURITY IN THE INTERNET ENVIRONMENT OF CHILDREN

Specialty: 3339.01 – “Methods and systems of information protection, information security”

Field of science: Technical

Sciences Applicant: **Sabira Safarali gizi Ojagverdiyeva**

Baku – 2024

The work was performed at the Institute of Information Technology of the Ministry of Science and Education of the Republic of Azerbaijan.

Scientific supervisor: Full member of ANAS, Doctor of Technical sciences, Prof.
Rasim Mahammad oglu Alguliyev

Official opponents: Doctor of Technical sciences, Assoc. Prof.
Yadigar Nasib oglu Imamverdiyev

PhD in Technical sciences
Vugar Yadulla oglu Musayev

PhD in Technical sciences
Lala Hekayat gizi Karimova

Dissertation Council ED 1.35 of Supreme Attestation Commission under the President of the Republic of Azerbaijan operating at the Institute of Information Technology of the Ministry of Science and Education.

Chairman of the Dissertation Council:
Full member of ANAS,
Doctor of Technical Sciences, Prof.
____________________ **Rasim Mahammad oglu Alguliyev**

Scientific Secretary of Dissertation Council:
Doctor of Philosophy in Technical Sciences, Assoc. Prof.
____________________ **Fargana Jabbar gizi Abdullayeva**

Chairman of the scientific seminar:
Doctor of Technical Sciences,

_____________________ **Ramiz Mahammad oglu Aliguliyev**

GENERAL CHARACTERISTICS OF THE WORK

The relevance of the topic and the degree of development. In the modern era of the Industry 4.0 revolution, the Internet has become a part of people's daily lives. With the proliferation of various Internet services such as e-mail, e-banking, e-commerce, social networks, online conferences, etc., individuals and companies carry out most of their daily activities online. As a result of these processes, a global digital environment formed for communication and other human activities. In addition to providing services to society, the Internet also creates serious problems and threats regarding information security. Such threats are understood as potential events, actions, and processes that could harm the reputation and interests of citizens[1].

Children, defined as individuals under the age of 18, are increasingly becoming active users of the Internet. According to the International Telecommunication Union (ITU), the number of children aged 5-17 using the Internet is rapidly increasing, reaching 1.75 billion in 2023, which accounts for approximately 83% of children in this age group[2].

The widespread use of mobile phones, tablets, and other digital devices has made the Internet accessible anytime and anywhere. While the Internet offers educational resources, entertainment, communication, and information, it seriously challenges children's information security. These challenges include:

– encountering inappropriate or harmful content;
– encountering vulgar language (profanity, insults, humiliation, hate speech, etc.);
– risk of personal unauthorized access and acquisition, administration, breach of privacy, cyberbullying;

[1] Prasad, R. Cyber security: the lifeline of information and communication technology / R.Prasad, V.Rohokale. – Cham, Switzerland: Springer International Publishing, –2020. – 274 p.

[2] Almost 80 per cent of people aged between 15 and 24 use the Internet, https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-youth-internet-use/

– Internet addiction (IA);
– the impact of using digital devices on the behavior, psychology, and physical health of children;
– problems related to the formation of information culture, etc.

Given that information on the Internet is collected without censorship, restrictions, or regulation, children are exposed to violence and socio-psychological threats every time they access online resources.

This underscores the urgent need for measures to ensure children's information security on the Internet (CIIS) and the safe use of beneficial Internet resources, making it one of the most pressing issues of the modern world.

In order to protect children from the harmful effects of the Internet, the ITU launched the "Children's Protection in Cyberspace" initiative in 2008[3].

In 2018, the Law "On the Protection of Children from Harmful Information" was adopted in the Republic of Azerbaijan[4].

This law defines measures to protect children from harmful information and regulates the relations concerning children's access to information appropriate for their age. According to the law, the dissemination of information to children that is suitable for a particular age group ("6-", "6+", "12+", "16+", "18+") and that depicts violence and ill-treatment as well as any content that contains cruelty, fear or erotic content is prohibited. "A Strategy for the Information Technology and Information Technologies of the Republic of Azerbaijan for the years 2023–2027" considers

[3]Child-Online-Protection, https://www.itu.int/es/myitu/News/2020/06/02/13/45/Celebrating-10-years-of-Child-Online-Protection

[4] Law of the Republic of Azerbaijan "On the Protection of Children from Harmful Information". [Electronic resource] / – Approved by the Decree of the President of the Republic of Azerbaijan No. 1310-VQ dated October 30, 2018 on the application of the Law of the President of the Republic of Azerbaijan. – Baku, November 21, 2018. URL: https://president.az/az/articles/view/30816

protecting children from threats, harmful information, and corruption on the Internet one of its targets[5].

The rapid proliferation of Internet services since the turn of the 21st century has spurred increased research on CIIS. These studies delve into critical issues such as the Internet's impact on children's health and psychological well-being, online gaming addiction, IA, gaps in the legal framework, encounters with cybercriminals, and exposure to harmful content. Importantly, these studies offer practical solutions for identifying and preventing the risks and dangers children face online.

Notable researchers in this field include S. Livingstone, L. Haddon, E.Y. Zotova, and G.U. Soldatova, among others. However, as the number of new virtual projects (Instagram, TikTok, Whatsapp, etc.) increases, so do Internet threats, leading to a rise in cyber victims. This necessitates the development of more reliable software tools, mechanisms, and new practical approaches to address CIIS.

The object and subject of the research. The object of the research in the dissertation is the information security of children when using the Internet. The subject of the research is the development of methods and algorithms for ensuring information security in children's Internet environments.

Purpose and responsibilities of the work. The dissertation aims to develop methods and algorithms using intelligent technologies to ensure children's information security in the Internet environment. The following research issues are set in order to achieve this goal:

- Analysis of the current situation and identification of existing problems in ensuring the information security of children in the Internet environment;
- Development of a conceptual model for ensuring the information security of children in the Internet environment;

[5] Decree of the President of the Republic of Azerbaijan on approval of the “Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023–2027”. [Electronic resource] / – Approved by Decree No. 4060 of the President of the Republic of Azerbaijan dated August 28, 2023. – Baku, August 28, 2023. URL: https://president.az/az/articles/view/60949

- Development of an algorithm for identifying vulgarity in web content;
- Development of a method for classifying malicious images;
- Development of a method for filtering malicious images;
- Development of a method for assessing children's Internet addiction based on log file analysis;
- Development of a multi-criteria decision-making method for selecting web content suitable for the children's age group;
- Development of an algorithm and method for managing children's access to information based on fuzzy logical inference.

Research methods. To solve the dissertation's problems, we used text mining technologies, natural language processing, machine learning, deep learning, neural networks, optimization, fuzzy logic theory, and multi-criteria decision-making methods.

The main provisions of the defense.

- Conceptual Model for Ensuring Children's Information Security in the Internet Environment;
- Algorithm for Detecting Vulgarity in Web Content;
- Method for Classifying Harmful Images;
- Method for Filtering Harmful Images;
- Method for Assessing Children's Internet Addiction Based on Log File Analysis;
- Multi-Criteria Decision-Making Method for Selecting Age-Appropriate Web Content;
- Algorithm and Method for Managing Children's Information Access Based on Fuzzy Logical Inference.

The scientific novelty of the work. The following contributions demonstrate the scientific novelty of this dissertation:

- A conceptual model has been developed to ensure children's information security in the online environment;
- An algorithm for identifying vulgarity in web content and a multi-criteria decision-making method for selecting content appropriate for children's age have been developed;
- A method for classifying and filtering harmful images has been proposed;

- A method for assessing children's IA based on log file analysis has been applied;
- An algorithm and method have been developed to control children's access to information using fuzzy logic deduction.

The theoretical significance of the work. Due to the development of scientific and methodological foundations in artificial intelligence, decision-making and fuzzy methods and algorithms enable the assurance and management of children's information security in the online environment at various levels (state, provider, corporate, and individual). The results obtained in the dissertation open up new opportunities for future research on children's internet safety. The findings of this study can be adapted to various contexts of information security.

The practical significance of the work. The results obtained in the dissertation are of practical significance and can be applied in the following areas:

- Enhancing web content moderation and filtering systems to improve the efficiency of online service providers;
- Increasing the capacity of cybersecurity agencies and Safer Internet Centers;
- Raising awareness among government agencies responsible for children's online safety about the dangers of the Internet;
- Incorporating into the educational process in secondary and higher education institutions, as well as other relevant contexts;
- More effectively managing children's access to information by integrating it into parental control programs;
- Ensuring children's access to age-appropriate and safe content in schools and libraries.

Realization and application of results. The main scientific and theoretical results of the dissertation work were included as important scientific results in the annual report on "Information security and cyber resilience" presented by the Department of Physical, Mathematical and Technical Sciences of the Academy of Sciences of the Republic of Azerbaijan in 2022 and 2023.

Approbation of the work and application of the results. The main scientific-theoretical and practical results of the dissertation work were reported and discussed at the same international and republican-level conferences, the list of which is presented below:

1. The International Conference on "Information Systems and Technologies: Achievements and Prospects", (Sumgayit 2018).
2. The 5nd Republican Conference on "Actual Multidisciplinary Scientific and Practical Problems of Information Security" (Bakı, 2019).
3. The 15nd International Scientific and Technical Conference on "Optical-electronic devices and devices in image recognition systems and image processing "Recognition — 2019", (Kursk 2019).
4. The 16nd International Scientific and Technical Conference on "Optical-electronic devices and devices in image recognition systems and image processing –"Recognition-2021"", (Kursk 2021).
5. The 3rd International Conference on "Information Systems and Technologies: Achievements and Prospects", (Sumgayit 2022).

Scientific publications. Based on the results of the dissertation, 17 scientific articles were published. Of these, 12 articles appeared in peer-reviewed journals recommended by the Supreme Attestation Commission under the President of the Republic of Azerbaijan, and five were published in the proceedings of international and national conferences. Additionally, 5 of the scientific articles were published in journals indexed in the Web of Science and Scopus databases.

The institution where the dissertation work is performed. The Institute of Information Technology of the Ministry of Science and Education of the Republic of Azerbaijan.

Structure and scope of the work. The dissertation consists of 178 pages, including an introduction, 4 chapters, a conclusion, and a list of cited literature with 197 names, 35 tables and 30 figures.

GENERAL CHARACTERISTICS OF THE STUDY

The introduction substantiates the relevance of the dissertation, identifies the research objectives and issues to be addressed, and highlights the scientific novelty and theoretical and practical significance of the results.

The first chapter, titled **“Analysis of the Current State and Existing Problems of Ensuring Information Security for Children in the Internet Environment,**” focuses on the contemporary challenges and solutions in this area. In the **first section of this chapter**, the global experience related to the safe use of the Internet by children, international programs, and laws adopted in various countries were analyzed. Furthermore, international initiatives addressing online child protection, including the functions of National Safe Internet Centers, were reviewed. Proposals and recommendations for establishing and effectively operating a similar center in Azerbaijan were developed [3, 10]. **In the second section,** the dissertation evaluates scientific studies and technologies related to CIIS. It offers a comparative analysis of specific methods and algorithms in the field, identifying the advantages of those employed in the research.**The third section** analyzes online risks faced by children in detail. It classifies various Internet threats and identifies the problems and consequences children encounter in the digital space.

The second chapter, **"Development of a Concept for Ensuring Children's Information Security in the Internet Environment,"** emphasizes the proposed concept's practicality and applicability. **The first section of the second chapter** discusses web content filtering issues. This section reviews international practices related to the topic, comparing automated mechanisms for imposing restrictions, filtering harmful web content, and removing inappropriate material. The levels of web content filtering (state, provider, corporate, and computer levels) are identified, and their distinct characteristics are highlighted [8]. **The second section of the second chapter** develops a conceptual model for a national intelligence system to address the issues of CIIS (figure 1) [1, 13].

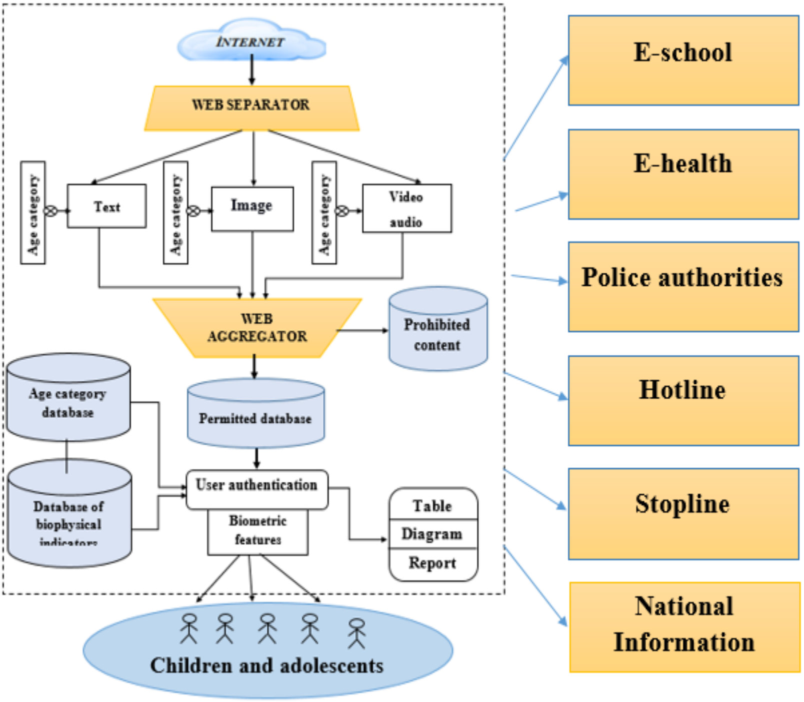


Figure 1. General architecture of the national intelligent system for ensuring children's information security

This model, crucially designed to integrate with the e-government platform, provides a comprehensive understanding of the dissertation's priorities. The significance of CIIS is underscored by its complex nature, which takes into account age differences, health capabilities, psychological states, and the relationships among these parameters. The development of a conceptual model for the system that ensures CIIS is deemed not just appropriate, but a significant step towards aligning with government initiatives.

The model depicted in figure 1 is based on an intelligent system composed of hierarchically organized components, such as a web separator, a veb-aggregator, user authentication, etc.

At the system's input, a web separator categorizes content based on data type (text, image, video) and children's age groups.

According to predefined conditions, prohibited web pages containing harmful content are detected. The information entering the "web aggregator" is then categorized into either the "prohibited data repository" or the "permitted data repository" based on the child's age group. The conditions are verified by referencing the "age category" and the "biophysical indicators database." In the next step, content is tailored to the child's age group by considering "user authentication" and "biometric features," ensuring appropriate web content is presented to the child.

The proposed national intelligence system is not just a standalone solution. It is designed to be integrated with e-education, e-health, e-police agencies, the National Information Center, and international projects (e.g., Hotline, Stopline). This broad integration ensures that the system is not just comprehensive, but also capable of addressing a wide range of issues. Additionally, it incorporates personalization features, enabling filters tailored to a specific child (considering the child's name, surname, age, biometric parameters, etc.).

The abundance of information and rapid data growth on the Internet poses significant challenges to children's access to helpful information. This is not just a theoretical issue, but a pressing concern that needs immediate attention. In light of this, **the third section of the second chapter** explores the challenges of big data in identifying beneficial web content for children. A conceptual model of a distributed system on parallel servers has been proposed to address the issue effectively. In distributed processing, data is processed in parallel by being distributed across multiple servers. This approach is beneficial for optimizing the efficiency of information management systems and timely obtaining information about the potential risk groups children may fall into in the future [7]

The third chapter, titled "**Developing Methods and Algorithms for Classifying and Filtering Harmful Web Content**," focuses on methods and algorithms for detecting, classifying, and filtering harmful web content (e.g., vulgar language, pornographic images) encountered by children online. **The first section has** developed a classification algorithm combining N-gram, TF-IDF, and Naive

Bayes methods to detect and clean vulgar language in web content [9, 16]. The algorithm is executed through the following steps:

Step 1. Data Collection. Because there is no database for vulgar words in Azerbaijani, a custom dictionary (*vulgarism_az*) containing approximately 300 words was created for experimental purposes.

Step 2. Preprocessing Data. Initial preprocessing of text significantly improves classification outcomes. Noise words were removed from the text.

Step 2. Feature Extraction. Vulgar words were detected in web pages (documents) using the N-gram and TF-IDF algorithms.

Problem Statement. Suppose a set of documents $D=(D_1,D_2,...D_n)$ is given, where n is the number of documents. Denote the of words occuring in D as $S_D=(s_1,s_2,...,s_m)$, where m is the total number of words. Each document D_i is represented as a vector in an dimensial Euclidean space, and the weight of a word in the document is calculated using the $w_{ik}=TF_{ik}\times IDF_k$.

Assume $C=(C_1,...,C_k)$ classes are known, to determine the probability of the i-th web page (D_i) belonging to the q-the class (C_q) the Bayers callisifier is used:

$$P(C_q\mid D_i)=\frac{P(D_i\mid C_q)P(C_q)}{P(D_i)} \tag{1}$$

here is $P(C_q/D_i)\;-\;D_i$ is the probability of the document belonging to (C_q) class (posterior), $P(D_i)$ – is the probabilit of D_i; $P(C_q)$ – is the probability of belonging to the C_q class (apriori), if $P(C_q\mid D_i)=\max\limits_{q=1,\dots,k}P(C_q\mid D_i)$, the $D_i\in C_q$ condition is satisfied. $P(C_q)$ is calculated as follows:

$$P(C_q)=\frac{\sum_{i=1}^{n}P(C_q|D_i)}{n} \tag{2}$$

$P(D_i\mid C_q)$ – is the probability that document D_i belongs to C_q.

The experiment is conducted in a Python program, and the constructed dataset is labeled with offensive words (0), jargon words and expressions (1), and swear expressions (2). Classification algorithms such as MultinomialNB, ComplementNB, GNB, and BernoulliNB have been used.

The method's effectiveness is evaluated based on a comprehensive set of metrics, including Accuracy, Precision, Recall, and F1-score. In the experiment conducted with N-gram+TF-IDF features, the GNB algorithm showed superior results (table 1), affirming the thoroughness of our evaluation process.

Table 1.
Results of classification based on N-gram+TF-IDF features using the GNB algorithm

Algorith	N-gram range	Class	Accuracy	Precision	Recall	F1-score
GNB	unigram	Humilating words	0.82	0.82	0.87	0.84
		Jargon words and phrases	0.91	0.91	0.83	0.87
		Profanity epxressions	0.95	0.95	1.00	0.98
GNB	N-gram+TF-IDF unigram	Humilating words	0.94	0.94	0.82	0.88
		Jargon words and phrases	0.80	0.80	1.00	0.89
		Profanity epxressions	0.93	0.93	0.93	0.93

The GNB algorithm recognized words from the "offensive words" class with 0.82 accuracy at the unigram level. When using the N-gram + TF-IDF feature, the algorithm identified words from the same class with 0.94 accuracy.

The comparative analysis results are shown visually in figure 2. The confusion matrix is displayed in figure 2(a), and the ROC curve is shown in figure 2(b).

In figure 2(a), the confusion matrix illustrates that most matrix elements are concentrated along the diagonal, with only a few misclassified points. Figure 2(b) shows the ROC curve, where the values across all classes in the dataset approach 1, visually indicating high performance.

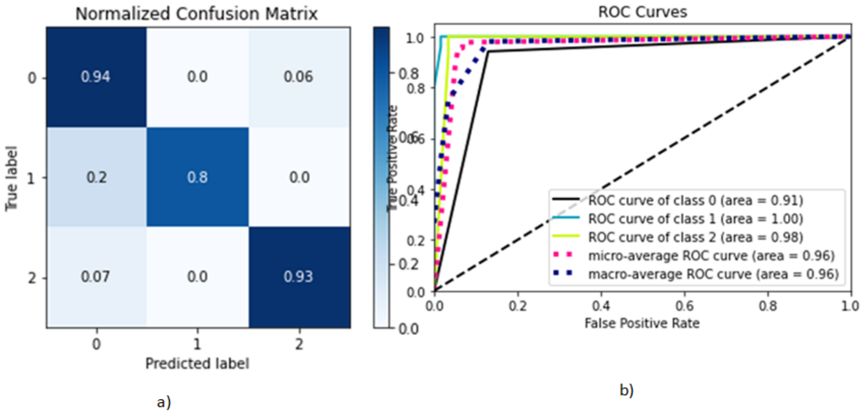


Figure 2. The confusion matrix (a) and ROC curve (b) of the GNB algorithm using N-gram + TF-IDF features.

In the second section of the third chapter, a method based on Convolutional Neural Networks (CNN) is proposed for detecting and classifying age-inappropriate malicious images encountered by children on the Internet [11].

Problem Statement: A new method is proposed to prevent children from encountering inappropriate images, which can accurately classify such images. For each class, a multi-layer neural network architecture is built to learn the texture patterns of unwanted image pixels, and it is executed sequentially in the following steps:

Step 1. Feature Extraction via Convolution Layer. The operation of extracting features from the image is performed using the following formula:

$$y_n^i = f_i(\sum_i y_m^{i\text{-}1} \otimes \omega_n^i + b_n^i) \tag{3}$$

where y_n^i – represents the future map of the image, i – denotes the number of layers, n indicates number of futures. $f_i()$ – is activating function. ω_n^i – is the filter that collects the features of the i-th layer,

b_n^i – is the bias, $\otimes$ – represents convolution operation. $y^{i-1}{}_m$ – is the matrix containing learnable weights that define the connection between neurons, m – is the number of the features in the $i-1$ layer.

Step 2. Data aggregation through the pooling layer and reduction of the feature map size. The pooling layer, with its simple reduction of the discreteness of the maps created by the convolution layer, divides the input data into regions, combines the values in the examined region, and produces only one output value. The maximum pooling formula is given as follows:

$$MaxPooling(X[i,j]) = \max Y[a,b],\ a,b \in R(i,j) \tag{4}$$

here is, $X[i,j]$ –is the value of the position of the object in the output map for the (i,j) position. $Y[a,b]$– is the value at the position of the object in the input map for the (a,b) positio. $R(i,j)$ – is the zone centered at the position of the object in the input function map for the (i,j) position. $MaxPooling()$ – is the maximization function that selects the dominant value from the elements within the local zone.

Step 3. Classification and prediction using a fully connected layer, a crucial component in the process. This layer leverages the high-level features extracted by the convolutional and pooling layers to classify or predict the output, engaging the audience in the classification process. Figure 3 shows the output parameters of the ChildNet model. The analyzed image has a size of 100x100 pixels, and the number 3 indicates that the image uses the RGB (Red, Green, Blue) format. The first two "fully connected" layers of the model consist of 4608 nodes (neurons), while the last "fully connected" layer contains n nodes. Here, n represents the number of classes, here $n=2$ is taken.We conducted the experiments in the Python programming environment. The model's effectiveness underwent testing on the 'NSFW – V1' and 'NudeNet' datasets. Both datasets consist of two classes: SFW (Safe For Work) and NSFW (Not Safe For Work). The training dataset includes 4000 images for each class (SFW and NSFW), while the test dataset contains 500 images from each class. We performed a comparative analysis of the ChildNet model against CNN and extended CNN models.

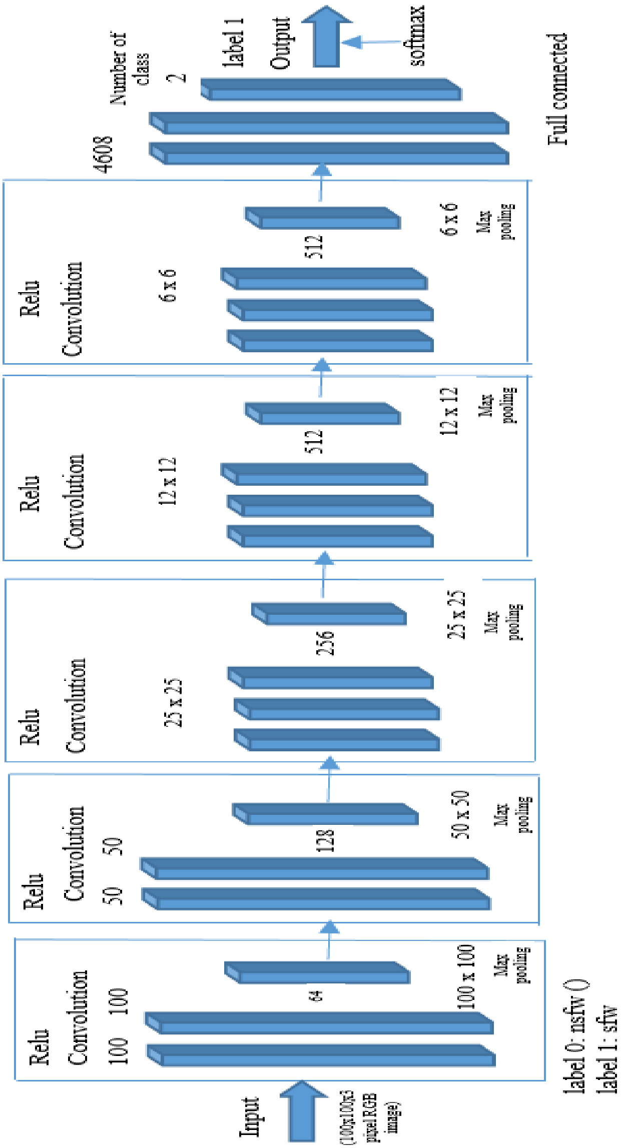


Figure 3. General diagram of the output parameters of the ChildNet model

During the training process, we experimented with different numbers of iterations, specifically 5, 10, 30, 50, 100, 300, and 1500. The model, utilizing the ReLU (Rectified Linear Unit) activation function, consistently achieved both low loss and high accuracy. This was demonstrated in the training and testing phases on a substantial dataset of 113,330 100×100 images, underscoring the robustness and reliability of the ChildNet model.

The third section of the third chapter introduces a novel method for filtering harmful images. Our approach, based on data sanitization technologies, is a unique and innovative way to detect, remove, or blur images unsuitable for child audiences, thereby ensuring CIIS [2, 6, 15].

Problem formulation: We start with a set of images X. Our task is to transform the sensitive data within these images into a form that cannot be recovered. To solve this problem, we propose an automatic encoder GRU (Generative Recurrent Unit) architecture to transform sensitive data. In this approach, we first input sensitive images into a latent vector, and the cleansing process occurs by generating images from the latent vector. As a result, blurring appears in the image. We implement this problem with the following algorithm:

Step 1. We predict fake data using the Logistic Regression (LR) block. We use two blocks—the Generator (autoencoder) and the Discriminator (logistic regression)—to control and cleanse children's access to harmful images in the online environment (figure 4).

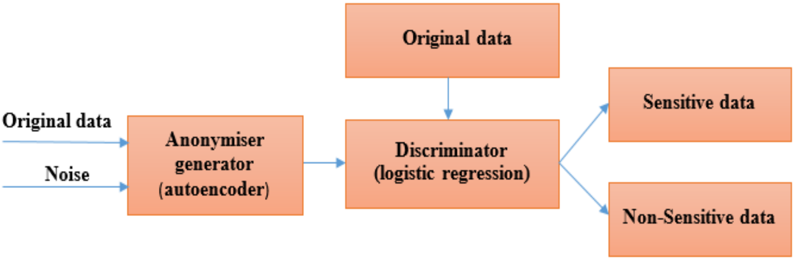

Original data
Original data
Noise
Anonymiser generator (autoencoder)
Discriminator (logistic regression)
Sensitive data
Non-Sensitive data

Figure 4. Data sanitization process

The autoencoder transforms sensitive attributes considered dangerous for children by adding noise to anonymize the input data, while the logistic regression performs classification. The LR block performs statistical forecasting in this research using one or more independent variables. We structure the GAN in a minimax format. The discriminator maximizes the obtained value, while the generator minimizes the value obtained by the discriminator.

Step 2. Data Transformation. In the initial data transformation, an autoencoder neural network hides sensitive information from children. This transformation prevents access to harmful web content and leads to the incorrect classification of sensitive data**.**

Let us assume that the transformation of the original x into $g(x)$ occurs through the floowing function:

$$g(x,u) \in G : X \times U \longrightarrow R^{2d} \tag{5}$$

here, g – represents transformation function, u – denotes the transformed data. The transformation of data causes certain losses and affects its utility. The task involves constructing a reconstruction algorithm that fulfills the following two objectives:

1. Minimizing the privacy risk:

$$\max_{u} \min_{v} f_{priv}(u,v) \tag{6}$$

2. Maximizing the utility risk

$$\max_{u} \min_{v} f_{util}(u,w) \tag{7}$$

The solution to the conflicting objective functions mentioned above is achieved by applying the following optimization function:

$$\min_{u}[\max_{v} f_{priv}(u,v) + \rho \min_{w} f_{util}(u,w)] \tag{8}$$

where, ρ is a constant number, the reconstruction shows the relative importance coefficient in terms of privacy.

Experiments were conducted in the Python program using a synthetic image dataset, a key component of our experimental setup. The sum of row elements with even numbers was labeled as sensitive data, and those with odd numbers were labeled as non-sensitive. When applying the proposed method to the data, the algorithm successfully identified sensitive data with low accuracy and non-sensitive data with high accuracy (table 3).

Table 3

Classification accuracy of the methods

		Rand	**PCA**	**PLS**	**LDA**	**The suggested method**
Non-sensetive date	Accuracy rate	0.6000	0.6150	0.6200	0.6200	0.6250
Sensetive date		0.4700	0.4750	0.4850	0.4850	0.4900

To evaluate the reliability of Rand, PCA, PLS, LDA, and the autoencoder, the program is executed 14 times on a synthetic dataset. Subsequently, a graphical representation based on the average results, in alignment with accuracy evaluation, is generated (Figure 5).

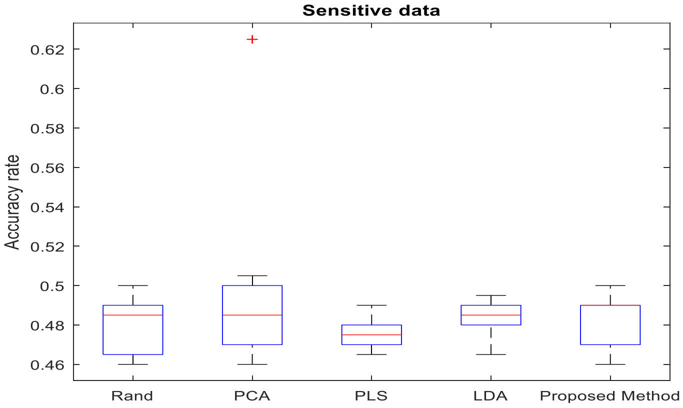


Figure 5. Descriptive graph of average values of accuracy metrics of data cleaning algorithms

Figure 5 illustrates the significant superiority of the proposed method over other algorithms, as evidenced by its remarkably small dispersion and well-represented density. This finding is of great importance in the field of IA management. Figure 6. underscores the method's unwavering and consistent performance, with accuracy rates maintaining a steady level of around 0.50. The robust management of sensitive data, with its strong and stable features, consistently achieves acceptable accuracy rates across various runs, instilling confidence in its reliability.

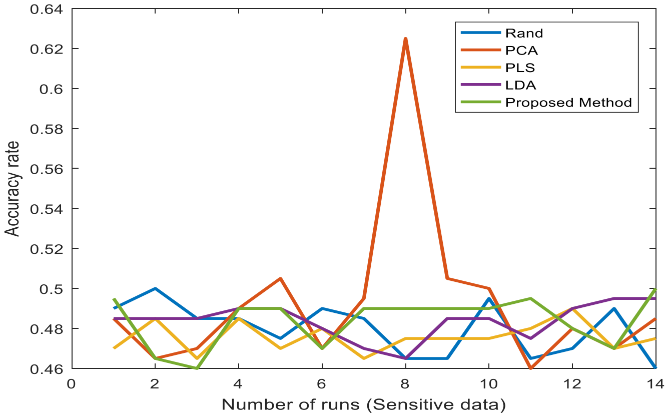


Figure 6. Accuracy dynamics of algorithms applied to sensitive data

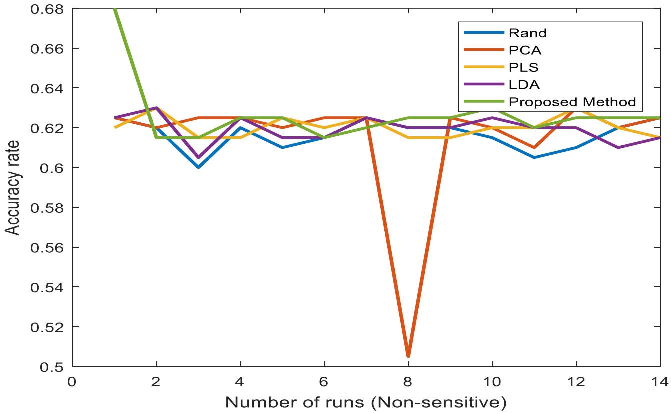


Figure 7. Accuracy dynamics of algorithms applied to non-sensitive data

Figure 7 compares the algorithms applied to sensitive data. The proposed method demonstrates more consistency, with accuracy scores fluctuating around 0.62. In contrast, other methods exhibit more significant variability in their accuracy scores.

The fourth chapter is dedicated to developing methods and algorithms for access control to harmful web content. **The first section of the fourth chapter** presents an analytical study of log files based on parameters such as the duration of children's Internet usage. It provides a systematic evaluation of the degree of IA using a weighted SVM formula [4].

Problem Statement. The goal is to assess children's IA by determining their level of dependence on the Internet. Classification is performed based on four categories (standard, low addiction, moderate addiction, and high addiction), and an algorithm is proposed for recognizing the addiction class.

Let us assume $S = \{(x_i, y_i, s_i)\}_{i=1}^{N}$ is a training data. x_i – represents the feature vector associated with the i-th data point, y_i – indicates the class to which the i-th data point belongs, s_i denotes weight coefficient of the $i-$th data point, N – refers to the total number of data points. The following formula gives the minimization of errors in classification:

$$\min_{\omega,\, b,\, \xi} \frac{1}{2}\|\omega\|^2 + C\sum_{i=1}^{N} w_i s_i \xi_i \qquad (9)$$

here ω – represents the weight vector of the hyperplane, b – is the correction term, w_i denotes the weight of the i-th data point. ξ_i – is the free variable for the i-th data point, and C – hyperparameter.

In the problem, when a data point is considered more important, its impact on the learned hyperplane can be increased by assigning a higher weight to this parameter. The following inequalities define the constraints for the weighted SVM formula:

$$y_i\left(\omega^t x_i + b\right) \geq 1 - \xi, \quad i = 1,\ldots,N\,,\ \xi_i \geq 0, i = 1,\ldots,N \qquad (10)$$

here, $t -$ represents the training dataset.

The experiments were conducted using a dataset of log files related to IA collected from internet users, with the "time spent on the Internet" parameter as the basis for the analysis[6] (table 4).

The conditional recorded time is considered relative to conducting the experiments, and several parameters can also be considered. The addiction criteria for children were defined, with the "highly addicted" class representing internet usage between 51-120 hours within a week, "normal" ranging from 1-15 hours, "low addiction" from 16-35 hours, and "moderate addiction" from 36-50 hours.

Table 4.

Recognition accuracy of points in the dataset

Clasifier	Correct Predictions	False Predictions	Total score
BernoulliNB	157	63	220
Logistic regression	194	26	
MLPClassifier	207	13	
SVM	203	17	
Proposed Weighted SVM	217	3	

As demonstrated in Table 4, the weighted SVM classifier emerges as the most accurate classification algorithm, delivering robust performance and precise predictions across all classes. Its exceptional accuracy is underscored by the fact that it correctly identified 217 out of 220 points, with only 3 instances of misclassification.

The second section of the fourth chapter meticulously outlines a multi-criteria decision-making method for selecting web content suitable for children's age groups [5]. The solution to the problem using AHP is a step-by-step process that ensures comprehensive consideration of all relevant factors.

*Problem Statement***.** Suppose it is required for children to access information from the Internet, and alternatives must be defined as harmless information (e.g., educational resources, safe

[6] Data set: “20150610_Internet Addiction dataset.sav”, 2015/, https:// https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4603790/

entertainment), educational content, entertainment content, news content, and harmful information (e.g., explicit or violent content).

The selection criteria for the alternatives are as follows: children under 6 years old, children older than 6 years, children older than 12 years, children older than 16 years, and users older than 18 years.

The decision is made by comparing the alternatives based on the given criteria. Figure 7 shows the decomposition of the proposed decision-making problem based on the hierarchy of criteria and alternatives.

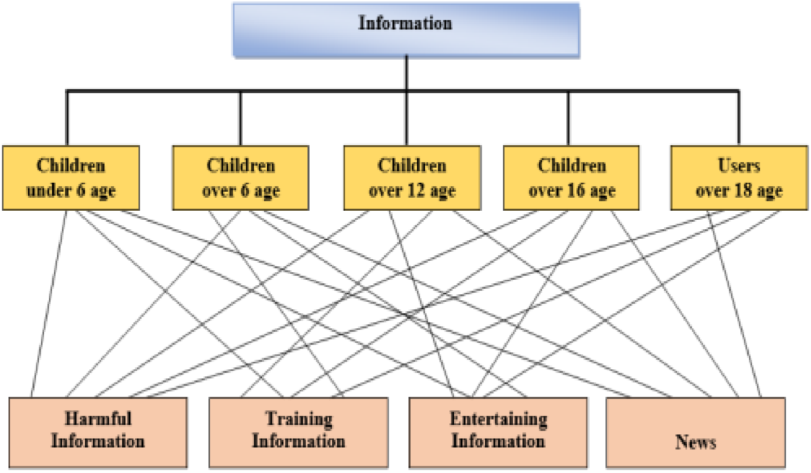


Figure 7. Decomposition of the decision-making problem based on the hierarchy of criteria and alternatives

Layer characteristics: Layer I – The crucial information source; Layer II – Set of criteria; Layer III – Alternatives. The problem is solved in the following sequence:

Step 1. *Creation of the comparison metric.* A pairwise comparison is performed among the five given criteria using Thomas Saaty's ranking scale, a tool that allows for the comparison of the relative importance of the criteria.

The scale consists of a range from 1 to 9. A relationship matrix is constructed with the following three characteristics between the criteria:

1. Diagonality: $S_{ii} = \overline{1,n}$

here i is an element of the matrice.

2. Inverse symmetry: $S_{ij} = \frac{1}{S_{ji}}$

Here, the elements of matrix S are symmetric with respect to the inverse, and the element S_{ij} represents the value obtained from the pairwise comparison between element i and element j.

3. Transitivity: $S_{ijg} \cdot S_{gj} = S_{ij}$

Here, the expression S_{ijg} indicates the value of the pairwise comparison between alternatives i and j based on the g criterion.

Step 2. Normalization of the matrix. The normalization matrix from Table 4 plays a key role in this step, ensuring that the elements of the comparison matrix are brought to the same scale. It is further described in Table 5.

*Step 3. Calculation of the Consistency Index***.** The formula for calculating the consistency index is straightforward, based on the pairwise comparisons conducted using the following formula:

$$CI = \frac{\lambda_{\max} - n}{n - 1} \tag{11}$$

here, $\lambda_{\max}$ – is the specific value, n – is the size of the matrix.

To calculate $\lambda_{\max}$ coefficient, the number next to the first criterion in Table 5 is multiplied by the average value of that criterion from Table 6. In Table 6, the values in the **'Sum'** column are calculated as the sum of the values in each row.

*Step 4. Calculation of the Consistency Vector***.** The consistency vector is obtained by dividing the corresponding element of the sum column in Table 6 by the corresponding value of the average value in the normalization matrix in Table 7.

Table 5.
Comparison Matrix According to the Ranking Scale of the Criteria

Age limit	Children under 6 years old	Children older than 6 years old	Children older than 12 years old	Children older than 16 years old	18 years old
Children under 6 years old	**1**	5	3	2	2
Children older than 6 years old	0.2	**1**	2	4	5
Children older than 12 years old	0.3	0.5	**1**	5	4
Children older than 16 years old	0.5	0.3	0.2	**1**	3
18 years old	0.5	0.4	0.25	0.3	**1**
Sum	**2.5**	**7.2**	**6.45**	**12.3**	**15**

Table 6.
Normalized Comparison Matrix According to the Criteria Ranking Scale

Criteries	Children under 6 years old	Children older than 6 years old	Children older than 12 years old	Children older than 16 years old	18 years old	Arithmetic Mean
Children under 6 years old	0.3947	0.6944	0.4651	0.1622	0.1333	0.3700
Children older than 6 years old	0.0789	0.1389	0.3101	0.3243	0.3333	0.2371
Children older than 12 years old	0.1316	0.0694	0.1550	0.4054	0.2667	0.2056
Children older than 16 years old	0.1974	0.0417	0.0310	0.0811	0.2000	0.1102
18 years old	0.1974	0.0556	0.0388	0.0270	0.0667	0.0771
Sum	1	1	1	1	1	1

Table 7.
Calculation of the Lambda Coefficient

Children under 6 years old	Children older than 6 years old	Children older than 12 years old	Children older than 16 years old	18 years old	**Sum**	Consistency vector
0.3700	1.1856	0.6169	0.2204	0.1542	2.5470	6.8846
0.0740	0.2371	0.4113	0.4409	0.3854	1.5486	6.5312
0.1233	0.1186	0.2056	0.5511	0.3083	1.3069	6.3558
0.1850	0.0711	0.0411	0.1102	0.2312	0.6387	5.7944
0.1850	0.0948	0.0514	0.0367	0.0771	0.4450	5.7742
Lambda						6.2680

*Step 5. Calculate the Consistency Index (CI) and Consistency Ratio (CR) Coefficients***.** Once the values of the lambda coefficient and the change are known, the consistency index (CI) is calculated using the formula (12). The following formula is used to calculate the consistency ratio (CR).

$$CR = CI / RI \qquad (12)$$

here, RI (Random Index) is the random consistency coefficient proposed by Thomas Saaty and is described with values as shown in Table 9.

Table 8.
Calculation of CI and CR coefficients

Number of criteria (n)	5
Consistency index (*Cİ*)	0.32
Consistency ratio (*CR*)	28%

Since the number of criteria is n, the value of RI is taken as 1.14 from the table above. Thus, the consistency ratio is calculated using formula (12) (Table 10).

Table 9.
Values of the consistency index

n	1	2	3	4	5	6	7	8	9	10
RI	0	0	0.53	0.88	1.12	1.25	1.34	1.40	1.45	1.48

Table 10.
Matrix of Alternative Selection and Ranking of Alternatives Based on the Matrix Multiplication Function

Alternatives	Children under 6 years old	Children older than 6 years old	Children older than 12 years old	Children older than 16 years old	18 years old	Weight	Score
Non-harming information	0.4691	0.4728	0.3741	0.1017	0.1194	0.3700	0.3830
Training information	0.1632	0.1802	0.3065	0.3507	0.2834	0.2371	0.2266
Entertainment information	0.2241	0.2201	0.1817	0.4032	0.3922	0.2056	0.2471
News infromation	0.1103	0.0938	0.0997	0.1130	0.1133	0.1102	0.1047
Harming information	0.0332	0.0331	0.0380	0.0313	0.0918	0.0771	0.0385

In the next stage, a matrix for selecting alternatives is constructed. The values obtained from the ranking of alternatives are entered into the calculation column in Table 9. In pairwise comparisons, the CR value should be close to 0 (CR < 0.1). The content that satisfies this condition is classified as harmful information. Our calculations consider content with a CR value between 0.0332, 0.0331, ..., 0.0385 harmful.

In the third section of the fourth chapter, we introduce a novel approach to controlling children's access to information. This approach utilizes a Fuzzy Logic Inference System (FLIS) [12, 17], offering a fresh perspective on the issue.

Problem formulation. The task of controlling children's access to information is a significant one. To tackle this, we consider several individual parameters for determining screen time.

First, we construct an architectural diagram for a web-content access control system in a internet environment for children (figure 8). The components of this architectural diagram are provided below:

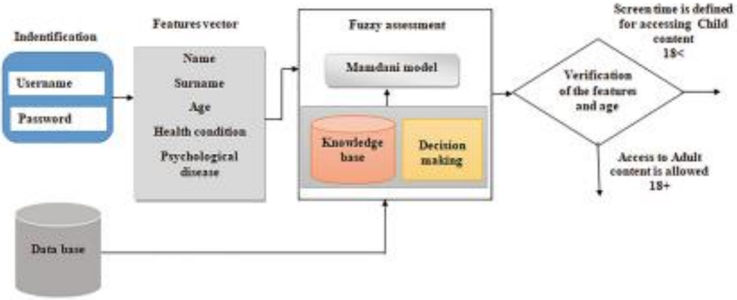


Figure 8. Architectural diagram of the system for controlling children's internet access

Identification. The process of recognizing the child to grant system access. This is typically achieved by the child entering their unique 'username and password', which serves as their digital identity within the system.

Feature vector This comprehensive data set contains vital information about the child, including their name, surname, age, health, and psychological state, providing a rich source for the system's operations.

Database. This repository is dedicated to storing detailed information about the child's diseases and psychological state from an early age, ensuring a comprehensive record for the system's operations.

Fuzzy evaluation. Based on the child's age, health, and psychological state, conditions for accessing web content are defined, and a knowledge base is formed.

Feature verification. The child's age determines their access to "Children's Web Content" or "Adults' Web Content."

In the study, the Mamdani fuzzy logic inference algorithm is used. This algorithm, which is a key component of the system, helps in making decisions based on vague, ambiguous, or imprecise information. It consists of the following steps:

Step 1: Fuzzification. In this step, the measurements of the primary parameters for determining safety are expressed in linguistic terms (e.g., 'young ', 'healthy ', 'happy') to handle imprecise data and converted into fuzzy numbers.

Determining input and output variables. The input variables for the children's information access control system are "child's age," "health," and "psychological state." The output variable is defined as "Internet content".

Defining fuzzy sets. Five fuzzy sets define the values of the input parameters for the fuzzy logic control system for children's information access: "very low" "low" "medium" "high" and "very high".

Defining membership functions. The degree to which a precise input value matches a specific linguistic term is evaluated, and this degree is assigned a value within the interval [0, 1]. The measurements for each input parameter are expressed in linguistic terms and converted into corresponding fuzzy numbers (table 11).

Table 11.
Values of the Fuzzy Triangular Membership Function

Exit parametrs	**Linguistic parameters**	**Interval values for the fuzzy triangular function**
Adult web-content (access not allowed)	Very low	[-0.4 0 0.2474]
Child content (Cannot exceed 10 min.)	Low	[0.0127 0.2447 0.491]
Child content (Cannot exceed 20 min.)	Mid	[0.251 0.504 0.742]
Child content (Cannot exceed 1.6 hour)	High	[0.497 0.718 0.996]
Adult web-content (acess allowed)	Very high	[0.747 0.9987 1.05]

In the research work, a triangular membership function is used (Figure 10).

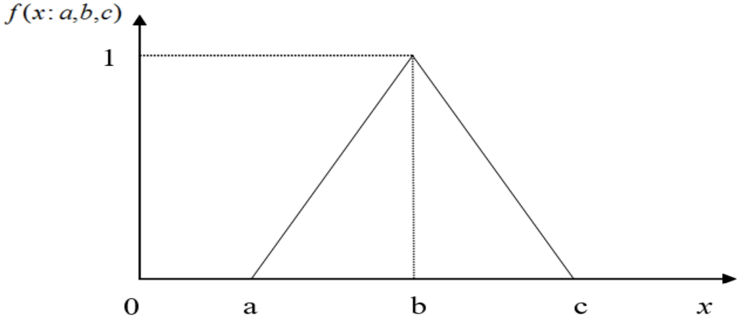


Figure 10. Triangular membership function

The membership function is defined by three parameters (a, b, and c)[7]: a – the point at which the membership function starts to increase from 0; b – the point at which the membership function reaches its highest – peak value;
c – the point at which the membership function decreases back to 0.

The values for the Internet content extraction block, crucial for understanding the membership function, are provided in Table 12.

Table 12.
Linguistic values of the Internet content extraction block

Linguistic value	Child age
Very low	4 years old
Low	6 years old
Mid	12 years old
High	16 years old
Very high	18 years old

Step 2. Establishing the knowledge Base for Rules. The creation of a knowledge base is a crucial first step in our process. This base, which focuses on child safety and screen time, is the cornerstone of the fuzzy inference system. It provides a framework for converting fuzzy

[7] Pamučar, D. S., Ćirović, G., & Božanić, D. (2019). Application of interval valued fuzzy-rough numbers in multi-criteria decision making: The IVFRN-MAIRCA model. Yugoslav journal of operations research, 29(2), 221-247.

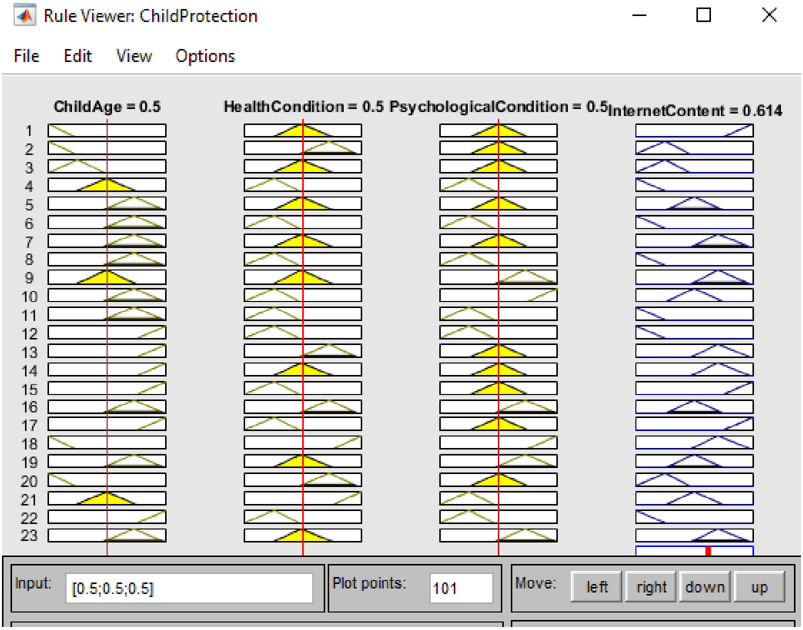
input sets into fuzzy output sets, with rules expressed in the familiar 'IF-THEN' format, mirroring human reasoning. The result is determined by a fuzzy set, a key component of our system.

Step 3. Extraction. At this stage, the power of our system comes into play. Decisions are made based on the fuzzy rules, with output parameters calculated for the given rules. Some of these rules are listed below, showcasing the system's ability to make informed decisions:

1. If (the child's age is 5, very low), (health condition is medium), and (psychological condition is medium), then the child may not access the "child content" for more than 10 minutes.
2. If (the child's age is 4, very low) (health condition is medium) and (psychological condition is medium), then the child cannot access the "child content."
3. If (the child's age is 6, low) (health condition is medium) and (psychological condition is medium), then the child can access the "child content" for 15 minutes.
4. If (the child's age is 12, medium) (health condition is low), and (psychological condition is low), then the child cannot access the "child content."
5. If (the child's age is 17, high) (health condition is high) and (psychological condition is medium), then the child can access the "child content" for 2 hours.
6. If (the child's age is 18, very high), (health condition is low), and (psychological condition is medium), then the child can access the "teen content."
7. If (child's age is 15, medium) and (health condition is medium) and (psychological condition is medium), then the child can access the "child content" for 1.5 hours.
8. If (the child's age is 16, high), (health condition is low), and (psychological condition is high), then the child cannot access the "child content."
9. If (the child's age is 17, high) (health condition is high) and (psychological condition is medium), then the child can access the "child content" for 2 hours.

10. If (the child's age is 18, very high) (health condition is low) and (psychological condition is medium), then the child can access the "adult content."

The blue triangles in Figure 15 represent the membership functions of fuzzy sets for input variables. The yellow triangles represent the fuzzy inference system's fuzzy output for each rule. In the lower right corner of Figure 15, the red line represents the graphical depiction of the system's final output. The shape of the red line represents the total membership degree for different output values.



[0.5;0.5;0.5]

101

Figure 15. Calculation of the Fuzzy Set via Aggregation

Step 5. Defuzzification. In this step, the fuzzy number is converted to a crisp value. Based on the fuzzy set, the best crisp value is determined by calculating the center of gravity using the following formula:

$$y_i = \frac{\int\limits_{\min}^{\max} x \ \mu_i(x)dx}{\int\limits_{\min}^{\max} \mu_i(x)dx} \tag{17}$$

here, y_i – is the result of deffuzzification for the value of the i -th output variable. d – is the accuracy coefficient of the value of the i -th output variable. μ_i – is the membership function corresponeding to the fuzzy set of E_i - $\min, \max$ – are the boundaries of the fuzzy set.

In the proposed expert system, the graphical representation of the data has been processed in Matlab's fuzzy inference system to review and evaluate information about children at risk (Figure 16).

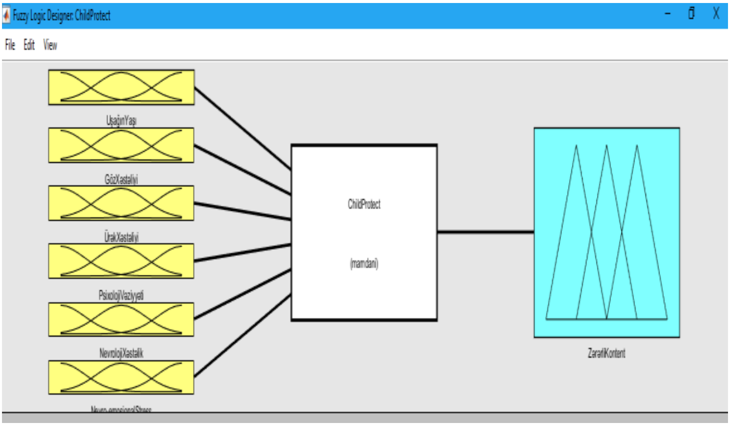


Figure 16. Screenshot of the ChildProtection software built on the Mamdani decision-making system

Figure 16 presents the visual interface of the ChildProtection software, a key player in assessing the level of protection for children from harmful content. The system actively processes input features, such as age, health, psychological condition, heart, eye diseases, and others, to form a comprehensive description of the child's overall condition. It then applies fuzzy rules to assess risks and makes decisions based on the evaluation.

RESULTS

During the development of the dissertation, the issues set out in the proposed topic have been solved, and the results obtained are outlined below:

1. The study of international programs, laws, and other official documents related to ESIC was comprehensive, encompassing the legal aspects, and scientific research and technologies in the field were analyzed comparably. This thorough approach led to developing robust recommendations for operating the National Safer Internet Center in Azerbaijan. The risks associated with children's information security in the Internet environment were identified and classified, and the problems encountered by children on the Internet and their consequences were determined and analyzed [3, 10, 14].
2. The conceptual model of the intellectual system for ESIC was developed. This model serves as a comprehensive framework for understanding and addressing the complex challenges of ESIC, providing a roadmap for future research and development in this critical area [1, 7, 8, 13].
3. The development of an algorithm based on the Bayes classifier for detecting vulgarities in web content is a testament to the innovative nature of this research. At the forefront of technological advancements, this method represents a significant step forward in content filtering [2, 9, 16].
4. A Deep Neural Network-based method was developed to classify harmful images in the ChildNet system. By leveraging the power of deep learning, this method significantly improves the system's ability to identify and filter out harmful images, thereby enhancing the safety of children using the Internet [11].
5. A method based on GAN for filtering harmful images was developed [6, 15].
6. A method based on weighted SVM for evaluating children's IA through log file analysis was developed [4].

7. A multi-criteria decision-making method based on AHP was developed for selecting web content suitable for children's age groups [5].
8. A method and algorithm for managing children's access to information based on fuzzy logic inference were developed [12, 17].

The following scientific papers have been published based on the materials:

1. Alguliyev, R., Ojagverdieva, S. **Conceptual Model of National Intellectucal System for Children Safety in Internet Environment**// International Journal of Computer Network and Information Security, – 2019, 11(3), – p.40-47. **(Scopus**)
2. Ocaqverdiyeva, S.S. **Verilənlərin sanitarizasiyasının bəzi aktual problemləri haqqında** // – Bakı: İnformasiya cəmiyyəti problemləri, – 2019. №1, – s. 99-108.
3. Ocaqverdiyeva, S.S. **Uşaqların İnternet təhlükələrindən qorunmasında qanunvericilikdən irəli gələn texnoloji vəzifələr haqqında** // – Bakı: İnformasiya Cəmiyyəti Problemləri, – 2019. №2, – s. 108-116.
4. Alguliyev, R.M., Abdullayeva, F.J., Ojagverdiyeva, S.S. **Log-File Analysis to Identify Internet-addiction in Children** // International Journal of Modern Education and Computer Science, –2021, 13(5), – p. 23-31. **(Scopus**)
5. Abdullayeva, F. Ojagverdiyeva, S. **Multicriteria Decision Making using Analytic Hierarchy Process for Child Protection from Malicious Content on the Internet** // International Journal of Computer Network and Information Security, –2021,13(3), –p. 52-61. **(Scopus**)
6. Alguliyev, R.M., Abdullayeva, F.J., Ojagverdiyeva, S.S. **Protecting children on the internet using deep generative adversarial networks** // International Journal of Computational Systems Engineering, –2020, 6(2), – p. 84-90.
7. Алекперова, И. Я., Оджагвердиева, С.С. **Проблемы безопасности детей и подростков в интернет и их**

решение с применением технологий больших данных // – Москва: Телекоммуникации, – 2020. №4, – с. 23- 31.

8. Ocaqverdiyeva, S.S. **Veb-kontentin filtrasiyası məsələləri** // – Bakı: İnformasiya Cəmiyyəti Problemləri, – 2020. № 2, – s. 80-88.
9. Abdullayeva, F., Ocaqverdiyeva, S. **Vulqarizmlərin maşın təlimi əsasında aşkarlanmasına bir yanaşma** // – Bakı: İnformasiya Texnologiyaları Problemləri, –2021. 12(2), – s. 89-98.
10. Ocaqverdiyeva, S.S. **Azərbaycanda Milli Təhlükəsiz İnternet Mərkəzinin yaradılması: problemlər və perspektivlər** // – Bakı: İnformasiya Cəmiyyəti Problemləri, – 2021. №1, – s. 138-19.
11. Alguliyev, R.M., Abdullayeva, F.J., Ojagverdiyeva, S.S. **Image-based malicious Internet content filtering method for child protection** // Journal of Information Security and Applications, – 2022, 65, – p.10312. **(Scopus, Web of science IF:3,8)**
12. Alguliyev, R.M., Abdullayeva, F.J., Ojagverdiyeva, S.S. **Child Access Control Based on Age and Personality Traits** // In International Conference on Computer Science, Engineering and Education Applications, Lecture Notes on Data Engineering and Communications Technologies. Warsaw, Springer, Cham, – 2023, 181, – p. 289-298. **(Scopus, Web of science)**
13. Ocaqverdiyeva, S.S. **Uşaqların informasiya təhlükəsizliyinin təmin olunması problemləri: konseptual model** // İnformasiya sistemləri və texnologiyalar: nailiyyətlər və perspektivlər beynəlxalq elmi konfrans, – Sumqayıt: SDU, – 15 noyabr, – 2018, – s. 391-392.
14. Ocaqverdiyeva, S.S. **İnternetdə uşaqların fərdi məlumatlarının qorunması vəziyyətinin analizi** // "İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" V respublika konfransı, – Bakı: İnformasiya Texnologiyaları, – 29 noyabr, – 2019, –s. 53-56.
15. Abdullayeva, F.J., Ojagverdiyeva, S.S. **Deep learning based data sanitization method for child protection on the Internet**// XV International Scientific and Technical Conference

"Optoelectronic instruments and devices in pattern recognition, processing and image systems (Recognition-2019)". Kursk, Russia, –14-17 may 2019, – p. 16-18.

16. Abdullayeva, F.J., Ojagverdiyeva, S.S. **Detection of vulgarities in web-content based on Naive Bayes algorithm** // Optical-electronic instruments and devices in pattern recognition and image processing systems. Recognition–2021. Kursk, Russia, – 14-15 septenber 2021, – p. 12-14.
17. Ocaqverdiyeva, S.S. **Azərbaycanda Milli Təhlükəsiz İnternet Mərkəzinin yaradılması: problemlər və perspektivlər** // – Bakı: İnformasiya Cəmiyyəti Problemləri, – 2021. №1, – s. 138-19.

The personal role of the claimant in the works published with co-authors:

[1] Participated in the research of proposed approaches and various security programs for protecting children from harmful information obtained from the Internet and developing a conceptual approach for the national intellectual system to ensure children's safety in the online environment.

[4] Played a pivotal role in formulating the research problem, developing the research methodology, and identifying relevant directions.

[5] The author was instrumental in formulating the research problem and investigating the acquisition of age-appropriate information for children in the online environment.

[6] Participated in formulating the research problem, the concept of data cleaning technology, its application areas, the investigation of approaches to data cleaning, the development of the article, and the proposal of a new approach for ensuring child safety.

[7] The author actively participated in investigating the application of big data technologies in the proposed system for children's information security on the Internet..

[9] Participated in formulating the research problem, investigating approaches and technologies for detecting harmful content, such as

vulgarisms in web content for the child audience, identifying relevant directions, and developing a new approach.

[11] Participated in investigating, detecting, and analyzing inappropriate images for children's age group as harmful information, obtaining data for experiments, identifying directions, and proposing a new approach.

[12] Participated in the investigation of applying restrictions on children's access to information in online environments, identifying directions, and proposing a new approach.

[15] Took a leading role in formulating the research problem, developing the article, and pioneering a new approach, inspiring the audience with innovative solutions.

[16] Participated in investigating the concept of vulgarism, its nature, and its harmful effects on the child audience, formulating the research problem and developing a new approach.

[17] Took an active role in formulating the research problem and developing a new approach, sparking excitement about the potential impact of the research.

The defense of the dissertation will be held on 7 February 2024 at 14^{00} at the meeting of the ED 1.35 Dissertation Council operating under the Institute of Information Technology of the Ministry of Science and Education of the Republic of Azerbaijan.

Address: Az 1141, Baku city, B.Vahabzadeh street, 9a

The dissertation can be viewed in the library of the Institute of Information Technology of the Ministry of Science and Education of the Republic of Azerbaijan.

Electronic versions of the dissertation and abstract are posted on the official website of the Institute of Information Technology of the Ministry of Science and Education of the Republic of Azerbaijan.

The abstract was sent to the necessary addresses on 28 December 2024.

Printed: 26.12.2024

Paper format: 60 × 84 $^{1/16}$

Volume: 39068 characters

Printing: 20 copies