JOURNAL OF EMERGING COMPUTER TECHNOLOGIES (JECT)

VOLUME: 1 ISSUE NO: 2 YEAR: 2021 PERIOD: JULY-DECEMBER

e-ISSN: 2757-8267

INTERNATIONAL, OPEN ACCESS, PEER-REVIEWED JOURNAL

http://dergipark.org.tr/ject

İZMİR AKADEMİ DERNEĞİ

JOURNAL OF EMERGING COMPUTER TECHNOLOGIES (JECT)

E-ISSN: 2757-8267

Volume :1 **Number:2** **Year:2021**

Indexing and Abstracting

Index Copernicus
https://journals.indexcopernicus.com/search/details?id=68795

Academia.edu
https://gkgkgkg.academia.edu/JournalofEmergingComputerTechnologies

Google Scholer
https://scholar.google.com/citations?user=n986qsIAAAAJ&hl=tr

Academic Resource Index (Researchbib)
http://journalseeker.researchbib.com/view/issn/2757-8267

ROAD
https://portal.issn.org/resource/ISSN/2757-8267

Asos Index
https://asosindex.com.tr/index.jsp?modul=journal-page&journal-id=2594

JOURNAL OF EMERGING COMPUTER TECHNOLOGIES

Volume: 1 **No:** 2 **Year:** 2021 **Period:** July-December

Head Office : İzmir
Type of Publication : It is published electronically twice a year, in June and December.
Owner : İzmir Akademi Derneği (İzmir Academy Association)

Editor : Dr. Muhammet DAMAR, Dokuz Eylul University, İzmir, Turkey.

Journal of Emerging Computer Technologies

Address : Büyükkale Mh. Kerimoğlu Sok. No:40-2 Tire / Izmir, TURKEY
Web : https://dergipark.org.tr/en/pub/ject
Email : journalect@gmail.com
Email : izmirakademidernegi@gmail.com

Journal of Emerging Computer Technologies publishes scientific/original research articles. It is published electronically twice a year, in June and December. It is an **international scientific refereed journal** that publishes articles written in **English**, and includes acedemicians from different countries in its boards. Uses "Double-Blind Peer Review" in reviewing processes. It has adopted the open access principle. No fee is requested from the authors for open access, processing, publication fee or otherwise. It is totally **FREE.**

Policies and Conditions

Publication Ethics

* The publishing processes of the Journal of Emerging Computer Technologies (JECT) are based on the unbiased production, development and sharing of information using scientific methods.
Refereed articles are studies that ensure the application of the scientific method and impartiality. In the realization of scientific production, all components of the publication process; publishers, editors, authors, referees and readers must comply with ethical principles.
* In this context, the publication ethics and open access policy of Journal of Emerging Computer Technologies (JECT), in line with the guidelines and policies published by the Committee on Publication Ethics (COPE) in open access (For example, the "Publication Ethics Committee (COPE) Code of Conduct and Journal Editors" The Best Practice Guidelines for “Code of Conduct and Best Practice Guidelines for Journal Editors” and “COPE Best Practice Guidelines for Journal Editors”) require that all components of the publication process comply with ethical principles.
* In situations such as manipulating and distorting the data used in the articles and using fake data are detected, this situation will be officially reported to the institution where the article author works and the article will be rejected. Our journal has the right to request the output files of the analysis results from the authors according to the feedback given by the editor and/or referees.

Publisher's Ethical Responsibilities

* The publisher of the Journal of Emerging Computer Technologies (JECT), is a non-profit person who takes care of the public interest.

* Journal of Emerging Computer Technologies (JECT) has been serving as an important journal in the field of social sciences under the management of the editorial board or editorial board since 2019.

* Members of the Editorial Board of Journal of Emerging Computer Technologies (JECT) are assigned for three years, taking into account the branches of social sciences. As the head of the Editorial Board, an editor and, depending on the situation, one or more assistant editors and field editors can be determined. A new member is appointed to replace the leaving member. The term of the expired member can be extended. According to the subject of the article, if necessary, the editor may send an article to experts who are not members of the Board of Editors (at least doctor's title) for review as a field editor.

Responsibilities of the Editorial Board of Journal of Emerging Computer Technologies (JECT)

* The Editorial Board of Journal of Emerging Computer Technologies (JECT) is responsible for every article submitted to the Journal of Emerging Computer Technologies (JECT) and even all processes after its publication, and the Editorial Board knows this responsibility. This responsibility, considering only the public interest in decisions made on issues related to the journal; it requires making decisions independently without considering personal gain. The relationship between the Publisher and the Editorial Board is based on the principle of independence, and all decisions taken by the editors are independent of the publisher and other persons and organizations.
* The Editorial Board of Journal of Emerging Computer Technologies (JECT) strives to continuously improve the journal and increase its publication quality.

* The Editorial Board of Journal of Emerging Computer Technologies (JECT) ensures that journal policies such as publication, blind refereeing, evaluation process and ethical principles are determined and implemented.

* The Editorial Board of Journal of Emerging Computer Technologies (JECT) protects the copyright of the article authors published in Journal of Emerging Computer Technologies (JECT).

* The Editorial Board of Journal of Emerging Computer Technologies (JECT) is responsible for taking measures regarding intellectual property rights, unscientific-unethical behaviours, plagiarism, sending (citation) gangs during the publishing process of articles and journals.

* The Editorial Board of Journal of Emerging Computer Technologies (JECT) prepares an "Author's Guide" containing the information requirements of the author (s) and a "Referee Guide" containing the information that referees will need during the evaluation phase, and updates it when necessary.

* The Editorial Board of Journal of Emerging Computer Technologies (JECT) determines policies to motivate the referees and the author (s).

* The Editorial Board of Journal of Emerging Computer Technologies (JECT) keeps the records of each article and correspondence related to the journal electronically or in print.

Ethical Responsibilities of Editor, Assistant Editors and Field Editors

* Editors strive to meet the information needs of referees, author (s), researchers, practitioners and readers, to provide feedback when necessary, to act according to the principles of clarity in matters that require correction and explanation during the publication process.
* While deciding on the publication of articles, editors take care that the articles are original and contribute to the scientific literature, readers, researchers and practitioners.
* While making positive or negative decisions about articles, editors take into account the original value of the articles, their contribution to the field, the validity and reliability of the research method, the clarity of the expression, and the journal's purpose and scope.
* Editors take the submitted articles to the pre-evaluation stage as long as they have no significant problems, consider positive referee suggestions, and do not change the decisions made by the previous editor (s) unless there is a serious problem.
* Editors implement the policies of blind review and evaluation process, which are among the publishing policies of the journal, keep the identity information of the referees confidential, and ensure that each article is evaluated objectively and in time.
* Editors send articles by taking into account the field of expertise of the editors and referees, and they support the impartial and independent evaluation.
* Editors consider whether there is a conflict of interest between editors, referees and author (s) for unbiased evaluation of the article.
* Editors seek to ensure that the referee pool consists of a wide variety and is constantly updated.
* Editors avoid unscientific reviews that do not follow academic etiquette.
* Editors ensure that the journal publishing processes are operated in accordance with publishing policies and guidelines, inform their field of duty in the process about the developments in publication policies, and prepare training programs when necessary.
* Editors are ineffective communication with everyone involved in the publishing process and hold meetings at regular intervals.
* Editors ensure the protection of personal data in reviewed articles; protect individual data of authors, referees and readers.
* Editors; They pay attention to the protection of human and animal rights in the articles, they care about documenting the explicit consent of the participants of the article, the approval of the ethics committee of the participants of the article, and they reject the article when they do not have permission for experimental research.
* Editors; they take precautions against misconduct. When there are complaints about misconduct, he makes an objective investigation and shares the findings on the subject.
* Editors ensure that errors, inconsistencies or misdirections in the articles are corrected.
* Editors protect the intellectual property rights of the published articles and defend the rights of the journal and the author (s) in case of violation. In addition, they take necessary measures to ensure that the content of published articles does not infringe the intellectual property rights of other publications; They do the authenticity-similarity check.
* Editors take into account the consistent criticism of the articles published in the Journal and give the right to reply to the author (s) of the criticized articles.
* Editors also consider studies with negative results.
* Editors examine the complaints submitted to the Journal and make the necessary explanations.

Ethical Responsibilities of Referees

* In the Journal of Emerging Computer Technologies (JECT) article evaluation process, the two-way blind refereeing principle is applied, in which the referees of the author (s) and the referees do not recognize the authors. The article evaluation forms and the notes stated on the text and the correction requests are forwarded to the author (s) by the editors through the journal management system. Referees who will evaluate the articles submitted to Journal of Emerging Computer Technologies (JECT) should bear the following ethical responsibilities:

* Referees should only agree to evaluate articles related to their field of expertise.
* Referees should make the assessment in neutral and confidentiality. In accordance with this principle, they should destroy the articles they have reviewed after the evaluation process, but use them after publication. Nationality, gender, religious belief, political belief and commercial concerns should not disturb the neutrality of the evaluation.
* When the referees understand that there is a conflict of interest, they should refuse to evaluate the article and inform the editors.
* Referees should make the evaluation in a constructive language in accordance with academic etiquette; Avoid personal comments containing insults and hostility.
* The referees should evaluate the article, which they accepted, within the time limit.

Ethical Responsibilities of Authors

Ethical responsibilities of the author (s) who apply for an article to Journal of Emerging Computer Technologies (JECT):
* Author (s) should not send an article that they have published elsewhere or sent to be published, or more than one article at the same time to Journal of Emerging Computer Technologies (JECT).
* Author (s) should submit an original article to Journal of Emerging Computer Technologies (JECT).
* The author (s) should correctly refer (cite) to the sources they use during the writing of the article in line with ethical principles.
* The names of persons who do not contribute to the article should not be written as authors, and it should not be suggested to change the order of the author of an article submitted for publication, to remove or add authors.
* Individuals who have a conflict of interest and a common interest related to the article for publication must be notified to editors.
* If information or raw data is requested from the author (s) during the evaluation process, they should submit the expected information to the Editors.
* The author (s) must document that the rights to use the data they use in their articles, permission for research-analysis or the consent of the participants on which they have researched.
* The author (s) should contact the editor to inform, correct or retract when they notice the error in the evaluation and early viewing or electronically published article.
* The author (s) have obtained the approval of the ethics committee for research that requires data collection by quantitative or qualitative methods such as experiments, questionnaires, scales, interviews, observations, focus group studies that require ethics committee decision; The name of the ethics committee, the date and number of the decision should be indicated on the first-last page of the candidate article and in the method section, and the document showing the ethics committee decision should be uploaded to the system with the application of the article. In addition, case reports should include information about obtaining informed consent / obtaining consent form in the article.
* The author (s) should present in the article the evidence that they adhere to ethical principles in the data collection process (such as obtaining permission from others to use documents such as scale, questionnaire, photograph). It should be stated in the articles that the copyright regulations for research and publication ethics and intellectual and artistic works are complied with. If the research was carried out on human and animal subjects, it should be reported that the research was carried out in accordance with international reports, guidelines, etc.
* Ethics committee approval is not required from the author (s) for review articles. However, in articles that do not require an ethics committee decision, it should be stated that an ethics committee decision is not required, on the first-last page and method section of the article.

Notifying the Editor of Non-Compliance with Ethical Principles

In the Journal of Emerging Computer Technologies (JECT), if an unethical situation regarding editors, referees, authors or an article that is in the process of evaluation, early appearance or an unethical situation is encountered, it should be reported to journalect@gmail.com.

Research Ethics

The following codes of ethics on research ethics contribute to research objectives, support values ??for collaboration, ensure researchers' responsibility to the public, provide credibility with public support, and reinforce various moral and social values:
1. The first rule is openness. In other words, the researcher has to share the data, materials, equipment, resources and findings he uses with the public. It should be open to criticism and new ideas.
2. Honesty and truthfulness: The researcher should not make up, steal, or misinterpret his findings. It must report results, methods, procedures accurately and not mislead colleagues, sponsors and the public. If he/she abuses research, it is also an unethical behaviour.
3. The researcher should not cause any harm to the object or subject of interest. Consequently, the researcher must respect people's privacy and secrets and should not use personal names unless permitted in his research. In addition, the researcher should not hide his identity.
4. Intellectual property: Patents, copyrights and other intellectual property must be respected. Unauthorized data, methods and results should not be used and contributors should be referenced.
5. Confidentiality: Confidential communications, personnel records, commercial and military secrets, patient records must be protected.
6. Being objective: biased experimental design, data analysis and interpretation should be avoided.
7. Integrity and consistency must be ensured.
8. Errors and omissions made due to carelessness should be avoided through a serious thorough examination of the work.
9. Social responsibility: Researches that may cause social damage should be avoided.
10. Discrimination: It should not be discriminated against by using gender, race, origin and other factors that are not related to scientific authority and integrity.
11. Relevant laws should be known and obeyed.
12. Caring for animals: Animals used during the research should be given due care and respect. Poorly designed and unnecessary animal experiments should not be done.

13. Protecting people: Risk and harm should be minimized in humanitarian research, human dignity, privacy and autonomy should be protected. Special precautions should be taken in research involving vulnerable persons with a child, developmental or cognitive disability, living in a nursing home, homeless or without legal status. The burden and benefits of research should be distributed fairly.
Planning and implementation of research on humans and animals, whose framework is drawn by national and international regulations and regulations, are the most important topics of research ethics. Research ethics is a concept that is mostly used for medical research, but undoubtedly, research conducted in social sciences is also within the scope of research ethics in a different dimension.

Obtaining Legal / Private Ethics Committee Permit

TRDIZIN EXPLANATION and DISCLOSURE of the Code of Ethics The articles related to the Code of Ethics in the criteria in the previous years were detailed in 2020 with explanations, assuming that permissions were obtained for studies requiring ethical committee approval in the field of research, and the issue of "including information about permission in the article" was added to the criteria.
Researches requiring Ethics Committee permission are as follows:
1) All kinds of research conducted with qualitative or quantitative approaches that require data collection from participants using a questionnaire, interview, focus group study, observation, experiment, interview techniques.
2) Use of humans and animals (including material/data) for experimental or other scientific purposes,
3) Clinical researches on humans,
4) Research on animals,
5) Retrospective studies in accordance with the law on the protection of personal data,
Also;
Stating that "Informed Consent Form" was obtained in case presentations,
Obtaining and indicating permission from the owners for the use of scales, questionnaires, photographs belonging to others,
Statement of compliance with copyright regulations for the intellectual and artistic works used
Retrospective ethics committee approval is not required for articles that have used research data before 2020, that have been produced from master's / doctoral studies (should be specified in the article), that have been published in the journal in the previous year, accepted but not yet published.
Researchers who are not members of the university can also apply to the Ethics Committees in their regions.
Also:
Whether an ethics committee approval and/or legal/special permission is required for articles to be published in journals should be stated in the article. If these permissions are required, it should be clearly presented from which institution, on what date and with which decision or issue number the permission was obtained.
If the study requires the use of human and animal subjects, the study should be included in an international declaration, guide, etc. It must be declared appropriate

Open Access Policy

Journal of Emerging Computer Technologies (JECT) has adopted the "open access policy" by considering the principle that increasing the global exchange of the knowledge generates useful results for humanity.Journal of Emerging Computer Technologies (JECT) is an "open access" journal the content of which is available to all users freely. Users can read the articles in full text, download, issue, print out and link to articles citing the journal without taking permission from the publisher or the author(s).
Our open-access policy is in line with the Budapest Open Access Initiative:
(http://www.budapestopenaccessinitiative.org/read).

https://creativecommons.org/licenses/by-nc/4.0/

CONTENT

Journal of Emerging Computer Technologies
Research Article
Received: *2021-01-18* | ***Reviewing:*** *2020-01-26* & *2021-03-16* | ***Accepted:*** *2021-03-17* | ***Online:*** *2021-03-17* | ***Issue Date:*** *2021-12-31*

Practical Evaluation on Serious Games in Education*

Slavica Mileva Eftimova
High School
SOU Jane Sandanski
Strumica, North Macedonia
meslavica@yahoo.com

Ana Madevska Bogdanova
Faculty of Computer Science and Engineering
Ss. Cyril and Methodius University
Skopje, North Macedonia
ana.madevska.bogdanova@finki.ukim.mk

Vladimir Trajkovik
Faculty of Computer Science and Engineering
Ss. Cyril and Methodius University
Skopje, North Macedonia
trvlado@finki.ukim.mk

***Abstract*— The arrival of the new learning methodologies is in response to the reality: new generations should learn in a different way. The so-called "Millennials" are looking for another kind of stimulus. Discussions for modernizing the curriculum include various solutions to retain students' attention and, in order to ensure that teachers learn how to act with a critical attitude, they will be confident and with the developed creative skills that they will need for success in the professional world in the future. The game based learning is more than providing educational games to students, it is about changing students' access to learning and their learning approach: the goal is to enjoy the learning process itself. This paper presents a methodological tool based on an evaluation framework for integration of digital games into education (MEDGE), expanded by adding additional information from the students, MEDGE+. The evaluation framework is used on three different approaches to the educational content: robot, micro: bit and playing quiz Kahoot. MEDGE+ presents better tool for the teachers in order to follow the student's interest when choosing appropriate educational games in the teaching process.**

Keywords—Serious games, critical attitude, games evaluation framework

I. INTRODUCTION

Today, the teacher abandons the role of a central figure, becomes a leader who guides the students through the learning process, enabling more learning styles, so that the student can move forward with his\her learning pace [1]. Students, on their part, use technology for communication, searching and finding information, expanding social experiences, and enjoying computer games on a daily basis [2]. The digital games (on their phones or computers) are played by students with a lot of energy and enthusiasm. This commitment is a challenge for the teacher - the learning process can be done through computer games. Students have transferable skills to share online research and access to many digital texts in a number of contexts. If digital literacy is encouraged throughout the teaching program, using positive language is necessary. By making such changes in the language teachers use, with the goal of becoming closer to their students' language, the students themselves will feel closer to the teachers and will understand the learning material more easily [3]. Technology offers a wide range of opportunities for developing learning experiences across a wide range of topics. If digital literacy is promoted through the curriculum, a positive language is required. By changing the language that teachers use, in order to be closer to the students, then the students themselves will feel closer with the teachers and will easily overcome the material.

II. RELATED WORKS

Confidentiality should be able to ensure that the data is only available to authorized users during the process and that it is not interfered by unauthorized people. Privacy is the most important security item in IoT because many devices can be integrated into IoT. It should be ensured that data received with a measuring device does not provide secure information to neighbouring devices. To ensure this privacy, advanced techniques and others, including key management mechanisms, should be developed and used [2].

It is essential to use wireless data transmission and to encrypt the information transferred between the nodes in order to keep it confidential. The most appropriate encryption algorithms and adequate key management systems are required to secure this data [3].

Wireless sensor networks have a large number of trust-based intrusion detection systems (IDS) that are used to defend against attacks. However, the effectiveness of IDS decreases in IoT due to the large amount of data produced in a short time. Meng et al. [4] proposed a Bayesian-based trust management method that incorporates traffic sampling into IDS under a hierarchical structure [5].

James King of Lulea University created an IoT network in his work in 2015 within the local network. Arduino used it as a gateway and collected and encrypted data from different devices and sensors. The encryption algorithm used is the Advanced Encryption Standard (AES) with both 128-bit and 256-bit key length [6]. Mahmudur Rahman, Bogdan Carbunar and Umut Topkara from Florida International University collects instant values from devices such as stopwatch, heart rhythm tracker and moisture meter used in fitness studies and transmits the IoT device to a web server remotely. In this study, FirstBeat is used as an encryption algorithm and Arduino Uno device is used as an IoT device. It also belongs to the IoT device from the webserver by taking the coordinate data, we can track the point we are at via GPS [6].

III. BACKGROUND

With carefully selected concepts and accompanying pictures that create a pleasant and creative atmosphere,

* This article is the extended version of the paper presented at the 16th International Conference on Informatics and Information Technology (CIIT 2019) on 10-12 May 2019.

Cite (APA): Eftimova, S. M., Bogdanova, A. M., & Trajkovik, V. (2021). Practical evaluation on serious games in education. *Journal of Emerging Computer Technologies*, 1(2), 21-24.

children learn more easily through various activities of games and tasks. The games often have a fantastic element that intrigue players and engage them in learning activities [4,5,6].

But in order to apply games in teaching, more conditions need to be met. According to the UNESCO framework, teachers should use educational (serious computer games) in education, preferably in accordance with the application of the teaching experience [3]. Teachers should have the following competencies:

- Using the Internet for online research;
- Using tools for making text and spreadsheets, making presentations;
- Using communication and collaboration tools such as emails, video conferencing and social networks;
- Application of ICT sources for curriculum development;
- Interest in continuing upgrading and improving the teaching content they teach and their teaching skills;
- Knowledge of the subject they teach to be appropriate for the age of the students;
- Have managerial and organizational skills;
- Knowledge of strategies that will help the student to gain in-depth knowledge such as:
    - Learning Collaboration;
    - Problem-based learning;
    - Project-based learning;
    - Activities based on project development;
    - Games and simulations;
    - Research experiments;
    - Case study;
    - Exercises;
    - Mentoring;
    - Evaluation.

What conditions should the school have in order to introduce educational games in teaching? The answer to this question divided in two parts:

- Provided technical equipment in the classroom and
- Teachers have to have appropriate digital competencies.

The word "competence" means knowledge or expertise in a given area [7]. Accordingly, digital competence is the ability to track, analyse, evaluate, generate and transmit information in digital format. This applies to desktops, laptops, smartphones and similar devices. Regarding the discussion of this term, there are various attempts to define definitions that are in use, as well as a few related names for it, such as information, the Internet or media competence. A person who is digitally competent will have more interlinked skills: knowledge of the basic principles of computer hardware, computer networking skills, the ability to engage in online communities and social networks. By digitizing human knowledge and developing digital technologies (mass production of devices that have access to the Internet). We can conclude that a digitally literate person will have practical knowledge of hardware and software, but also different kind of knowledge that they did not have in the last century. Computer literacy is often considered today as the ability to use the computer programs for some less complex practical tasks or the ability of individuals to effectively use the computer. Digital competence, or in other words, digital literacy, is considered to be as important today as reading and writing. Digital devices are starting to be used from an increasingly young age, but this does not help much young people to develop the skills they need for further personal and professional upgrading. Digital competence is far more than just accepting new technologies and using social media in order to create some content.

Today, digital literacy is almost equally necessary to attain personal and professional ambitions. It allows seemingly complex tasks to be performed in a much simpler and more efficient way and with better results. It is necessary to focus attention on the way the students use devices in extracting knowledge.

Digitalization and inroads have already led to major changes in our daily lives and our world in terms of information and work. However, these numerous changes have not yet become clearly visible and understandable to us. For this reason, it is particularly important to pay attention to large volumes of new information and to all innovations. To do this, it is necessary to have a sufficiently high level of digital competence.

As far as the technical equipment of the schools is concerned, as a first requirement is that there is an Internet connection and at least one laboratory with a certain number of computers, preferably connected in a local network. Possession of additional tools and equipment can greatly enrich hours with certain activities. The LEGO Mindstorm EV3 Robot [8] and micro:bit tools [9] are used in practical case studies.

IV. THE CASE STUDY

In order to conduct this evaluation, the evaluation framework for integration of digital games into education (MEDGE) was used [10], expanded with two new questions, thus MEDGE+.

The following questions were answered by several professors at the "Jane Sandanski" High School:

- Is the game easy to use? (EASY)
- What is the educational goal of the game? (VAL)
- Does the game adapt to educational goals? (ADT)
- Pleasure / acceptance of the game by students? (QoE)
- What is the teacher's subjective opinion about the game? (SUB)
- What is the motivation of students to adopt the material? (MOT)

In order to achieve better motivation for the students when applying serious games, two questions were added, where the students were asked the following questions (MEDGE+):

- Through the game, I will easily overcome the material (EL);
- Through the game, my motivation for material adoption (MS) will increase.

The following scale of responses was offered:

I totally agree (5). I agree (4), I am neutral (3), I disagree (2), I completely disagree (1).

A. *Case Study 1 - LEGO*

A class in high school using a memory game (with the help of the LEGO Mindstorm EV3 Robot) [8].

Teaching unit: One-dimensional arrays;

Type of lesson: lecturing;

In order to get the students interested as much as possible on this thematic unit, a memory game in Python was used through simulation of robotic games. Preparing for this guide: LEGO Mindstorm EV3 Robot is the tool used for this game. A robot with specific parts is built in the instructions for building the LEGO Mindstorm Education Core Set. The goal and the game is to build the main body for the robot (base unit) and the color sensor.

Effects

Computer Science (Python) - This lesson will help students understand the use of an array, from an abstract concept to a point where they actually understand how the color storage works in random order. Students will be introduced to the random functions used to generate colors.

Exercise

Create a program that will put random colors in sequence, and then the robot will repeat (express) the order of colors. The student must remember the colors and show colors on the card to the robot sensor in the same order as given. In the end, the robot announces whether the study of time wins or not.

Reflection

Students learned how to store colors in arrays and to check if the generated colors are the same as shown in front of the sensor. They can also make different versions of this program by counting a score and saving other type of data. Based on a poll conducted after playing this game, the following results were obtained, given in the Fig1:

	EASY	VAL	ADT	QoE	SUB	MOT	EL	MS
robot	2,5	3,4	5	3,8	4,4	4,6	**4,4**	**4,1**

Fig. 1. Review of robot responses, MEDGE+

B. *Case Study 2 - KAHOOT*

Teaching unit: Basics in programming with C++ Type of lesson: Kahoot quiz to check the acquired knowledge on the topic Introduction to programming in C ++.

Kahoot [11] is a formative learning tool that uses quizzing technology, discussions and surveys. The principle of work is basically a game in which the whole class participates in real time. For the preparation of this class, a quiz with 10 questions was developed, which examines the gained initial knowledge in programming in C ++, which is necessary to start programming the simplest tasks in C ++.

Exercise

Students get the link and join the game.

Reflection

The class with Kahoot was filled with excitement and euphoria like no previous one. The competitive spirit was at the highest level. After the quiz was conducted, questionsthat were incorrectly answered were discussed. The students asked after each teaching unit (or at least after completing a theme) to have a time dedicated to competing with the Kahoot Quiz**.** Based on the conducted survey after playing this game, the following results were obtained, given in the Fig2:

	EASY	VAL	ADT	QoE	SUB	MOT	EL	MS
Kahoot	4,6	5	5	5	4,7	5	**4,8**	**4,7**

Fig 2. Review of Kahoot responces, MEDGE+

C. *Case Study 3 - MICRO:BIT*

A class in high school using a micro:bit [9] to verify acquired knowledge of algorithms with a branched structure.

Teaching unit:

Algorithms and programming;

Type of lesson:

Algorithms and their representation. In order to hold this lesson, the OOU Sando Masev Strumica was visited, where, with the help of the British Council, the school owns 30 micro:bit devices [12]. At this class, the application of the algorithm with a branched structure was presented, realized practically with the micro:bit device.

Exercise The acquired experiences were used for introduction into the branch structure. Other approaches were introduced to explain algorithms with a branch structure. The students were able to solve other examples.

Reflection

By using the micro:bit, the programming becomes clearer, closer and more attentive to the students. The survey by MEDGE+ has produced the table in Fig 3.

	EASY	VAL	ADT	QoE	SUB	MOT	EL	MS
micro:bit	4,3	5	5	4,5	4,2	5	**4,8**	**4.5**

Fig.3. Review of micro: bit responces, MEDGE+

The evaluation methodology MEDGE+ produces the net presented in Fig.4. It gives graphical representation of the game/tool acceptance in the three case studies.

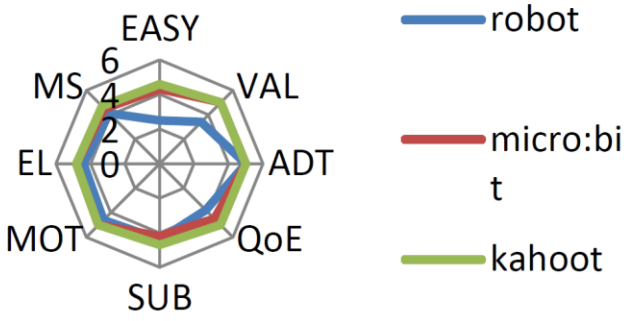

Fig4. Evaluation of the explored games with MEDGE+

V. DISCUSION

In this part a discussion of the three case-studies is given. At the lesson of one-dimensional strings, the good sides were: greater interest and curiosity towards something new, resulting in increased interest in learning and interest in research through additional sources for the new concepts. The negative sides were that the use of robots in teaching requires additional costs, one robot is a not enough for a group of 24-30 students. Another point is the programming language - in order to use the robot in the teaching process, another programming language was needed, and not the one that is studied in the regular classes. The good sides in the realization of classes using the Kahoot quiz for repeating the material for the basics of programming were: initiating a competitive spirit, raising awareness of teamwork, getting quick results for the correct answers and showing greater interest in understanding the reasons of choosing the wrong answers. Also, all students answered the same questions at the same time and there was no fear of consequences if wrong answer was submitted.

In the third case study, the algorithms for a branched structure with micro: bit was introduced. The positive side was this new approach to learning algorithms. It was more interesting to the students because of the visualization and the ease of use. One disadvantage of using micro:bit in high schools is that following the curriculum, micro:bit can be applied only at the beginning of the programming courses because the latter material is more complex.

VI. CONCLUSION

The introduction of games in IT teaching is a very positive experience [13,14,15], but of course, the realization of each of these serious games and tools has positive and negative aspects.

In this paper, following the evaluation methodology [10], MEDGE+ was introduced that can give even more insight when choosing an appropriate educational game in the teaching process. We have explored three case studies, and used the MEDGE+ methodology to measure the acceptance of the given games and tools.

The performed analysis was done over three different games: robot simulation, Kahoot and micro:bit coding. It showed that all three activities positively influenced the process of adopting new knowledge and knowledge testing, while the greatest satisfaction and motivation according MEDGE+ achieved the quiz Kahoot. The extension of the methodology [10] considered the inclusion of the student's opinion, contributing to the teacher's decision which games/tools should be chosen in the educational process.

The use of games in teaching obviously has many advantages, and as a future work, more examples of games and tools will be evaluated using the information provided by MEDGE+.

REFERENCES

[1] L. Phipps, V. Alvarez, S. de Freitas, K. Wong, M. Baker, and J. Pettit, "Conserv-AR: A Virtual and Augmented Reality Mobile Game to Enhance Students' Awareness of Wildlife Conservation in Western Australia", Proceedings of the 15th World Conference on Mobile and Contextual Learning (mLearn 2016), Sydney, Australia, vol. 1, pp. 214-217, 2016

[2] H.A. Spires, "21st century skills and serious games: Preparing the N generation," in L.A. Annetta, Serious educational games. Rotterdam, The Netherlands: Sense Publishing, 2008

[3] United Nations Educational, Scientific and Cultural Organization, unesco ict competency framework for teachers, 2011;

[4] P. Fotaris, T. Mastoras, R. Leinfellner, and Y. Rosunally, "Climbing Up the Leaderboard; An Empirical Study of Applying Gamification Techniques to a Computer Programming Class," Electronic Journal of e-Learning, vol. 14, no. 2, pp. 94-110, 2016.

[5] T.M. Connolly, E.A. Boyle, E. MacArthur, T. Hainey, and J.M. Boyle, "A systematic literature review of empirical evidence on computer games and serious games," Computers & Education, vol. 59, pp. 661–686, 2012.

[6] J.C. Burguillo, "Using game theory and Competition-based learning to stimulate student motivation and performance," Computers & Education, vol. 55, no. 2, pp. 566–575, 2010

[7] Digital competence https://europass.cedefop.europa.eu/resources/digital-competences , 15.12.2018;

[8] Lego education, https://education.lego.com, 25.02.2019;

[9] Micro:bit, https://microbit.org/code/, 25.02.2019;

[10] Maja Videnovik , Ana Madevska Bogdanova , Vladimir Trajkovik, "Serious games evaluation methodology", Proceedings of ICERI2018 Conference 12th-14th November 2018, Seville, Spain;

[11] M. Videnovik, L. Kionig, T. Vold, and V. Trajkovik, "Testing framework for investigating learning outcome from quiz game: A Study From Macedonia and Norway," in 17th International Conference on Information Technology Based Higher Education and Training (ITHET), pp. 1-5, IEEE, 2018

[12] Materials by teacher Biljana Nikolova, OO Sando Masev Strumica, 15.12.2018;

[13] Gamestorming, https://gamestorming.com/category/games-for-problem-solving/, 12.02.2019;

[14] M. Popescu, S. Arnab, R. Berta, J. Earp, S. De Freitas, M. Romero, I. Stanescu, and M. Usart, "Serious games in formal education: discussing some critical aspects," in Proceedings of 5th European Conference on Games-Based Learning, Athens, Greece, pp. 486–493, 2011

[15] Immersing, addaptive learning https://www.ixl.com, 12.02.2019

Journal of Emerging Computer Technologies
Research Article
Received: *2021-02-22* | ***Reviewing:*** *2021-03-03* & *2021-03-26* | ***Accepted:*** *2021-03-26* | ***Online:*** *2021-03-30* | ***Issue Date:*** *2021-12-31*

Digital Twin Based Disaster Management System Proposal: DT-DMS

Özgür Doğan
Department of Computer Enginnering
Muğla Sıtkı Koçman University
Muğla, Turkey
ozgurdogan3@posta.mu.edu.tr

Oğuzhan Şahin
Department of Computer Enginnering
Muğla Sıtkı Koçman University
Muğla, Turkey
oguzhansahin3@posta.mu.edu.tr

Enis Karaarslan
Department of Computer Enginnering
Muğla Sıtkı Koçman University
Muğla, Turkey
enis.karaarslan@mu.edu.tr

***Abstract*— The damage and the impact of natural disasters are becoming more destructive with the increase of urbanization. Today's metropolitan cities are not sufficiently prepared for the pre and post-disaster situations. Digital Twin technology can provide a solution. A virtual copy of the physical city could be created by collecting data from sensors of the Internet of Things (IoT) devices and stored on the cloud infrastructure. This virtual copy is kept current and up to date with the continuous flow of the data coming from the sensors. We propose a disaster management system utilising machine learning called DT-DMS is used to support decision-making mechanisms. This study aims to show how to educate and prepare emergency centre staff by simulating potential disaster situations on the virtual copy. The event of a disaster will be simulated allowing emergency centre staff to make decisions and depicting the potential outcomes of these decisions. A rescue operation after an earthquake is simulated. Test results are promising and simulation scope is planned to be extended.**

Keywords*— *Smart city, Digital Twin, IoT, IoT Connectivity, Digital transformation, Cyber-Physical Systems, Disaster management

I. INTRODUCTION

Metropolitan cities are becoming more crowded and their transportation, telecommunication, electricity networks, and natural gas networks are becoming more complex day by day. Natural disasters are a reality and these big cities have to be ready for pre and post-disaster situations. Turkey is no exception.

The number of natural disasters such as earthquakes and their destructiveness are expected to increase in the future. The most recent earthquake in Elazığ showed that disaster management practices and the tools to train staff for pre and post-disaster situation are not sufficient. The fundamental elements of post-disaster interventions were late and communication infrastructures collapsed.

Digital twin technology can be used as a solution. Digital twin can be defined as the bridge between the physical and virtual world. The data received from physical assets are transferred to the digital twin. Digital twin technology can be used to build smarter buildings and infrastructures like transportation, telecommunication, electricity, and natural gas networks. Such a solution should be developed before any crisis to allow emergency staff to be trained to meet the surmountable challenges of a natural disasters, especially an earthquake.

In the next section, fundamentals of digital twin solution are explained. Related works are provided in the third section. The proposal of the system is explained in the fourth section followed by the implementation in section five. The results and conclusions are included in final section.

II. FUNDAMENTALS

A. Disaster Management

Today's technology is not yet sufficient in predicting when disasters will take place [1]. However, today's technology is sufficient to supply means which enables us to take measures before and after the disaster to reduce catastrophic effects of any incident on human lives and property. Disaster management can be used for the following:

- Prevent and reduce the impact of the disasters,
- Respond to the events in a timely, fast and effective manner.
- Create a new and safer environment for the victims.

Disaster management can be examined as pre and post disasters. In pre-disaster, the following actions can be taken to reduce risk and harm.

- Determining regions that exist on the fault line,
- Informing and raising awareness of the society about disaster hazard and risk,
- Improving disaster management capacity and capability,
- Installation of IoT devices in the buildings and in the critical infrastructures such as transportation, telecommunication, electricity and natural gas networks.

In a post-disaster situation, timely response by allocating resources to the most affected areas is one of the most critical aspects to reduce human suffering and number of casualties. In this context, gathering current information becomes the most crucial thing. Information/data about the affected areas can be gathered by using the IoT devices that are installed during the pre-disaster period. This data can be transferred to the rescue teams and could be used to allocate scarce resources to the most affected and areas to facilitate efficient relief operations. Drones, satellites, and similar devices could also be used to collect information on conditions of the disaster region. The data that is collected from these devices could be

Cite (APA): Doğan, Ö., Şahin, O., & Karaarslan, E. (2021). Digital Twin Based Disaster Management System Proposal: DT-DMS. *Journal of Emerging Computer Technologies*, 1(2), 25-30.

used in making decisions about the establishment of the following:

- number and nature of rescue teams,
- kind of equipment,
- mode of transportation,
- location of the relief camps.

There is a need for a decision support system that combines all the collected data and helps in producing an insight into the disaster.

B. Smart City and Smart Nation

The migration of people to metropolitan cities for certain reasons makes management difficult in those regions. The population in cities in Europe was 50 percent in 1950, now it is over 75 percent [2]. The urban population will be approximately 6.7 billion in 2050 [3]. As a result of this urbanization, systems generate big data. The smart city [4] concept is about collecting these data and using them in decision support systems. Technologies such as IoT, AI (artificial intelligence), cloud computing [5], and blockchain [6] can be used. These all can be used to form a smart nation as shown in Fig. 1.

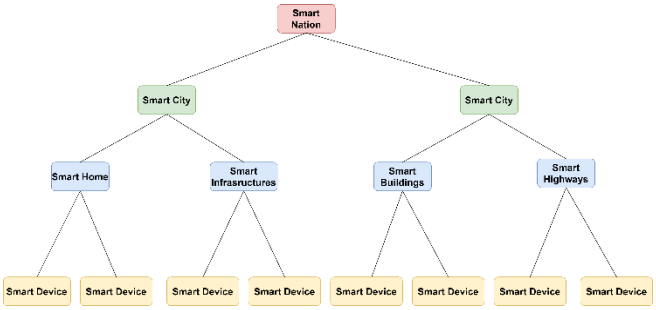

Fig.1: Smart Nation Concept

C. Digital Twin

Digital twin technology is based on creating a virtual copy of an object, process, or human being in a virtual world. This virtual copy is kept current with continuous incoming data.

The concept of digital twin is not new. This technology was used for the first time in the 1960s by NASA (National Aeronautics and Space Administration). NASA has created virtual duplicate systems for a space mission to test its equipment and estimate potential costs. The "digital twin" term was introduced in 2002 by NASA's advisor Dr. Michael Grieves. It was also developed in the US Air Force and applied to the aircraft body models in 2013. Digital twin technology has become one of the most promising technology trends with the widespread usage of IoT (Internet of things).

Essential simulations and examinations to test a system, mechanism or a tool can be done easily with this technology reducing potential costs and manpower as well as avoiding harms to human life. The digital twin consists of three main concepts; physical assets, sensors, and virtual copy. The virtual copy displays the data from the IoT devices as 2D/3D or non-visual. Decision-making process of humans or machines can become easier using this display.

As open-source software has become more popular in the computer industry [7], it is also sensible to use a variety of these open-source protocols, frameworks, and tools for digital twins and IoT. Eclipse Ditto, AllJoyn, and IoTivity frameworks can be used. Communication protocols that can be used are; MQTT (Message Queue Telemetry), AMQP (Advanced Message Queueing Protocol), COAP (Constrained Application Protocol), XMPP (Extensible Messaging and Present Protocol) [8] and RabbitMQ.

D. Digital Twin Communication

One of the most important features of humankind is the ability to communicate with each other. Life proceeds in a certain order with the help of this communication. Roads, buildings and infrastructures in the smart city which were created exist individually in the system. They can act by each other's feedback.

The connectivity mostly occurs between IoT devices. The number of IoT connected devices increased by 285% since 2015 and the number of these devices is around 38.5 billion [9]. The sectors such as manufacturing, logistics, health, agriculture, and automotive use IIoT (Industrial Internet of Things) often. Disruptions, delays, and stoppages of jobs can cause substantial losses. Therefore, communication is an important component for the IIoT. In smart cities, the communication must not be interrupted between digital twins for the sustainability of management and life.

The fourth period of the industry has begun (Industry 4.0) which is based on CPS (cyber-physical systems). CPS is a hybrid system that has a physical and virtual environment in communication with each other. In CPS everything is interconnected wirelessly. Smart factories, autonomous cars, quadcopters, etc. are substantial examples of CPS.

These devices are in constant communication with each other and also connected to the internet. There are lots of different ways to make these connections such as RFID, ZigBee, WPAN, WSN, DSL, UMTS, GPRS, WiFi, WiMax, LAN, WAN, 3G, etc [10]. These types are given in Table 1.

Table 1. IoT Connectivity Types

Type	Radio Frequency	Range	Data Transfer Speed
Bluetooth	2.4 GHz-2.5 GHz	0,5 m-100 m	$\leq 24Mbps$
Wi-Fi	2.4 GHz-5 GHz	45 m-91 m	$\leq 250Mbps$
Zigbee	860 Mhz-2.4 GHz	10 m-100 m	$\leq 250Kbps$
GPRS	Diff. in each reg.	8 km-40 km	56-114 Kbps
3G	Diff. in each reg.	8 km-40 km	0,8-2 Mbps
4G	Diff. in each reg.	8 km-40 km	0.2-1 Gbps
5G	Diff. in each reg.	8 km-40 km	$\geq 1Gbps$

III. Related Works

There are mainly touristic implementations in the smart city concept. Newcastle, Dubai, Qatar and Singapore started to form their digital twins. Qatar and Singapore have the aim to use digital twins in a touristic sense. In the three-dimensional virtual copy of the city, it also aimed for people to go on the streets and see touristic places [11].

However, using digital twins for disaster management is rare. Digital twin technology is used for so many different projects and studies in the literature. [12-15]. For example, it

is used for controlling floods in Newcastle by monitoring the amount of water on the roads [16].

However, there is a lack of academic studies that can be used for better solutions and standardization. Only a recent study [17] addressed this idea and proposed a "disaster city" concept. Our study is an attempt to develop a proof of concept how to implement Digital Twin on a disaster management setting where further studies can be built upon. This prototype will address a variety of disaster (earthquake, storm, fire etc.) types and collect data from a variety of sources such as electricity, natural gas and communication infrastructures of the buildings are planned to be controlled.

IV. System Proposal

The proposed system aims to develop essential measures for pre- and post-disaster environment by performing various simulations on a virtual copy. These measures include information on as buildings, transportation, telecommunication, natural gas and electricity networks. This system could also be used real-time to collect data following a disaster to decide how rescue operations are managed by understanding of the occupancy rate of critical facilities such as hospitals.

Digital twin architecture is shown in Fig. 2. Sensors collect data from the physical world and sent it to the virtual environment which is stored in the cloud. Continuous flow of data is the most essential and crucial requirement of the system. This data can be collected from many sources such as IoT sensors, social media, data resources from government and municipality. This data will be stored in database systems on the cloud.

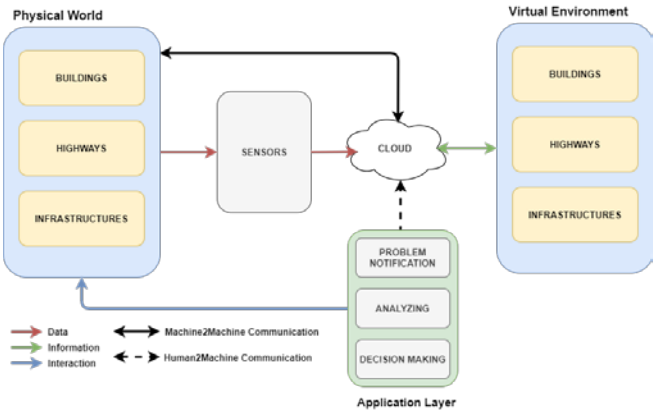

Fig. 2: Digital Twin Architecture

There are two main actors of the system that are the staff at the disaster management centers and the rescue teams. Organizations can use this system from the rescue centers and the teams can use these data during the intervention. Also in the post-disaster scenario; buildings and rescue center information of the relevant streets can be checked by clicking on the icon of buildings and the rescue center. In the infrastructures section, electricity, water, and telecommunication facilities can be inspected. A timeline button is used in order to analyze the effects of the disaster on time. The system can be run in two modes:

- Education mode: Based on the decision of the management staff, the simulation is made and possible outcomes are reported.
- Estimating mode: Decision support system runs in several different choices and tries to find the best decision for the best outcome.

The action diagram of the system is in Fig 3. Diagram consists of three components; server, IoT Devices, and UI (User Interface). When the user starts the system, the data can be received from realtime data or stored data. The system may have dynamic live data obtained instantly from the IoT devices. If not, previously-stored simulation data is loaded and relevant scenarios are run on this data.

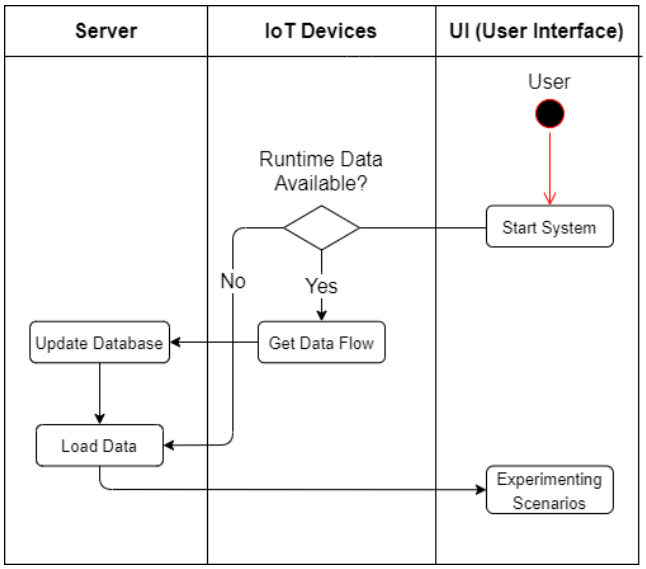

Fig. 3: Action Diagram of the System

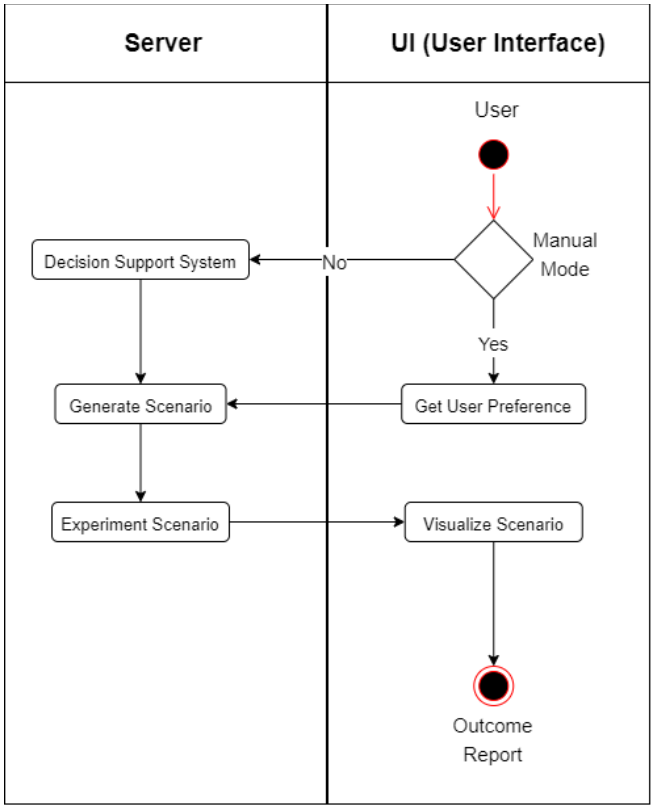

Fig. 4: Action Diagram of Experimenting Scenarios

Experimenting scenarios are given in detail in Fig. 4. This can be done in two ways. In manual (education) mode, choices are made by the trainee. Users' preferences are taken and according to these preferences, appropriate scenarios are created. Otherwise, the decision support system creates different scenarios by itself and decides which result is most effective in these different scenarios. Also, the decision support system can make changes to the real IoT devices. At the end of the scenario, a report is presented which includes how many people survived, state of buildings, and infrastructures. Depending on these, the effectiveness of the scenario is analyzed.

The graphical user interface is also one of the issues to be considered. It can be examined under two main options: 3D or 2D. All of these approaches have important advantages and also limitations as well. Some of the strengths and weaknesses of each system are highlighted on Table 2. 3D modelling requires too much computational power and time. Since our sources are limited, it also was not considered appropriate. Given all these situations, 2D model was chosen for the system.

Table 2. GUI Types

	Advantages	Disadvantages
3D	More accurate modelling	Difficult to model very large areas
	Suitable for buildings, bridges	Need more computational power
2D	Large areas easily to build	Hard to model complex structures
	Low computational power	Less detail, low accuracy

V. IMPLEMENTATION

The implementation aims to educate the emergency centre staff. The system prototype for the education mode is made where an earthquake scenario was implemented. The event of a disaster will be simulated; the situation from the beginning of the earthquake in a timeline can be analyzed by users. Post-earthquake infrastructure data can also be examined. Possible outcomes of the decisions will be reported accordingly.

A prototype simulation is implemented as a proof of concept on an ordinary laptop with 8 GB RAM, 256 GB SSD,6 GB GTX 1050 Ti and an Intel i5-8300H 2.3 GHz CPU.

The incoming and stored data must be visualized to make it more meaningful. MapBox is selected to create the map service [18]. Conditions of the buildings and the roads are marked by visualization elements.

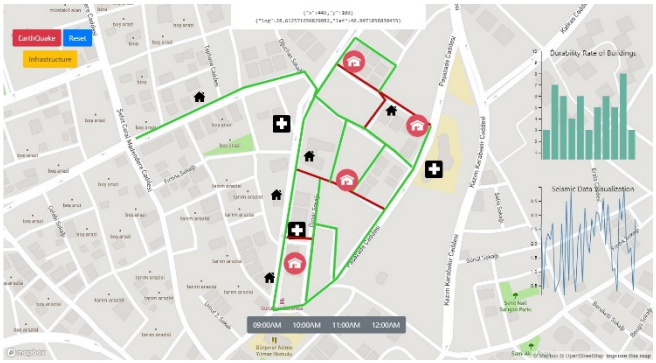

Fig. 5: Post-Disaster Prototype Interface

The user enters the map service and reaches the necessary live pre-disaster visualizations and analysis about buildings, rescue centres, and roads. The prototype interface is shown in Fig. 5. The user can switch to the map style containing the infrastructure information and analyzes the water, electricity, and communication infrastructures. This prototype interface is shown in Fig. 6. The environment is simulated with instant data.

Fig. 6: Post-Disaster Prototype Interface for Infrastructures

The simulation environment is used to show the status of the buildings, infrastructures (such as communication, power, electricity, water and natural gas) and the roads in a timeline after the disaster. The most appropriate directions/paths for the rescue teams are given by the decision support system. The system recommends the following:

- Number and type of rescue teams according to the civilization density and the status of the buildings.
- The best live-saving scenario(s) with the most appropriate paths from the best available rescue centre to the wreck.

Simulation provides the users several options with potential success rates. When a decision is chosen, the outcome is also shown in the simulation. Then a rescue team vehicle departs from the rescue centre and goes from the shortest and safest way to save the people. The outcomes of this decision is presented to the user.

A system that uses artificial intelligence algorithms such as Breadth-First Search (BFS) [19] and Uniform-Cost Search (UCS) [20] is being developed. This will help in recommending the best options which will help rescue teams to identify better alternative to save lives.

Social media such as Twitter is an important communication channel in times of emergency. The iniquitousness of smartphones enables people to announce an emergency in real-time. Because of this feature, more agencies (i.e. disaster relief organizations and news agencies) are interested in programmatically monitoring Twitter. It's not always clear whether a person's words are announcing a disaster. An NLP (Natural Language Processing) model [21] which detects whether the tweets are fake or not was developed. Transfer learning, particularly models like Allen AI's ELMO, OpenAI's Open-GPT, and Google's BERT [22] is being used to smash multiple benchmarks with minimal task-specific fine-tuning. These are also providing the rest of the NLP community with pre-trained models that could easily (with less data and less compute time) be fine-tuned and implemented to produce state of the art results. Hence, in this project, it is decided to use Google's pre-trained BERT model.

Google's pre-trained BERT model is preferred in this project. The dataset used for training the model consists of two components. The first is the text of the tweet. The other is the estimation of whether the tweet is about a real disaster (1) or not (0). This dataset was produced using a CSV file obtained from Kaggle [23]. This file contains information; a unique identifier for each tweet, the location the tweet was sent from, and a particular keyword from the tweet. This dataset contains 7613 tweet texts. The size of the dataset is relatively small compared to modern deep learning models. Hence, the data was split into an approximately 80:10:10 ratio for the training set, development set, and test set respectively. This breaks up of 6091 training examples, 1522 validation examples, 1522 test examples. Binary cross-entropy is chosen as a loss function of this model. AdamW is chosen for optimizer of the model, because it optimizes the learning rate used in gradient descent.

VI. RESULTS

The results of the simulation as part of our first experiments are promising. The simulation covered a small area, therefore the amount of data was limited. Building and infrastructure data was entered manually to the database. The "Earthquake Activity in Istanbul in the Last Year" dataset [24] from IBB open data was used. However, for a digital twin; the data must be provided dynamically from social media and IoT sensors. The system will be better when such an environment is provided. Using live data is to be implemented in a future study. Moreover, also the NLP model result were promising. The dataset was pretty simple and small which is not good for BERT model. It is trained just 4 epochs. After training section, accuracy on test data is about 67% that is not considered as. Increasing the size of dataset and making necessary optimizations for better performance of model is considered as a future study.

VII. CONCLUSION

Natural and manmade disasters are an inevitable part of our daily lives and governments, institutions, local authorities and individuals must be prepared for such an event. The necessary measures before the disasters are key to reduce the damage on property and the number casualties. "Earthquakes don't kill people, buildings do" expression should not be forgotten.

Disaster management is an important issue to be addressed and digital twin technology can make it easier for us. The concept is still new for many countries, but it is expected to become mainstream within the next five to ten years. Simulations in the virtual copy can help us to learn and prepare the necessary precautions. After the disaster, even seconds are important for saving lives. It is pretty crucial to intervene immediately. Digital twins can also help us with this issue.

Test results are promising and simulation scope is planned to be extended. The simulation results are to be used to have the idea of taking necessary precautions on housing, transportation, telecommunication, natural gas, and electricity networks. The real-time data after a disaster is planned to be used on deciding how rescue operations to be carried out, figuring out the fullness/sturdiness ratio of the mission-critical buildings like hospitals.

Future works will include running this whole system in the cloud, as the amount of data from sensors and social media will increase gradually. These sensors will be placed on the buildings and infrastructures like electricity, transportation, telecommunication, and natural gas. This study will be extended to the city level and a central intelligence in which all regions facing the risk of earthquakes will be considered.

REFERENCES

[1] Coppola, D. P. (2006). Introduction to international disaster management. Elsevier.

[2] Caragliu, A., Del Bo, C., & Nijkamp, P. (2011). Smart cities in Europe. Journal of urban technology, 18(2), 65-82.

[3] United Nations, "World Urbanization Prospects: The 2018 Revision

[4] Su, Kehua, Jie Li, and Hongbo Fu. "Smart city and the applications." 2011 international conference on electronics, communications and control (ICECC). IEEE, 2011.

[5] Brian, H., Brunschwiler, T., Dill, H., Christ, H., Falsafi, B., Fischer, M., & Kaiserswerth, M. (2008). Cloud computing. Communications of the ACM, 51(7), 9-11.

[6] Nofer, Michael, et al. "Blockchain." Business & Information Systems Engineering 59.3 (2017): 183-187.

[7] Tan, L., & Wang, N. (2010, August). Future internet: The internet of things. In 2010 3rd international conference on advanced computer theory and engineering (ICACTE) (Vol. 5, pp. V5-376). IEEE.

[8] Madalli, D. P., Barve, S., & Amin, S. (2012). Digital preservation in open-source digital library software. The Journal of Academic Librarianship, 38(3), 161-164.

[9] Sun, H., Wang, C., & Ahmad, B. I. (2017). From Internet of Things to Smart Cities: Enabling Technologies. Chapman and Hall/CRC.

[10] S. Smith, IoT Connected Devices to Triple to Over 38 Bn Units, Juniper Research, 2020. [Online]. Available:https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020

[11] Farsi, Maryam, et al., eds. Digital Twin Technologies and Smart Cities. Springer, 2020.

[12] Aydın, Ö., & Karaarslan, E. (2020, June). Covid-19 Belirtilerinin Tespiti İçin Dijital İkiz Tabanlı Bir Sağlık Bilgi Sistemi. Online International Conference of COVID-19 (CONCOVID).

[13] Yukcu, S., & Aydin, Ö. (2020). Maliyet Düşürme Yöntemi Olarak Dijital İkiz. Muhasebe Bilim Dünyası Dergisi, 22(3), 563-579

[14] Fan, C., Zhang, C., Yahja, A., & Mostafavi, A. (2021). Disaster City Digital Twin: A vision for integrating artificial and human intelligence for disaster management. International Journal of Information Management, 56, 102049.

[15] Yükçü, S., Aydin, Ö., & Koçakoğlu, Ü. Ö. (2020). Bağimsiz Denetimde Dijital İkiz Uygulamasi. Mali Cozum Dergisi/Financial Analysis, 30(161).

[16] Ham, Youngjib, and Jaeyoon Kim. "Participatory Sensing and Digital Twin City: Updating Virtual City Models for Enhanced Risk-Informed Decision-Making." Journal of Management in Engineering 36.3 (2020): 04020005.

[17] Damjanovic-Behrendt, V., & Behrendt, W. (2019). An open source approach to the design and implementation of Digital Twins for Smart Manufacturing. International Journal of Computer Integrated Manufacturing, 32(4-5), 366-384.

[18] CADENAS, Cecilia. Geovisualization: Integration and Visualization of Multiple Datasets Using Mapbox. 2014.

[19] Beamer, Scott, Krste Asanovic, and David Patterson. "Direction-optimizing breadth-first search." SC'12: Proceedings of the International Conference on High Performance Computing, Networking, Storage and Analysis. IEEE, 2012.

[20] VERWER, Ben J.. H.. ; VERBEEK, Piet W.. ; DEKKER, Simon T.. . An efficient uniform cost algorithm applied to distance transforms. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1989, 11.4: 425-429.

[21] Collobert, Ronan, et al. "Natural language processing (almost) from scratch." Journal of machine learning research 12.ARTICLE (2011): 2493-2537.

[22] Adhikari, A., Ram, A., Tang, R., & Lin, J. (2019). Docbert: Bert for document classification. arXiv preprint arXiv:1904.08398.

[23] (2020). Real or Not? NLP with Disaster Tweets. https://www.kaggle.com/c/nlp-getting-started/data.

[24] İtfaiye Daire Başkanlığı, Earthquakes That Happen in the Last One Year Around Istanbul [İstanbul Çevresinde Son Bir Yılda Gerçekleşen Depremler], 2020. [Online]. Available:https://data.ibb.gov.tr/dataset/istanbul-da-son-bir-yilda-gerceklesen-depremler

Journal of Emerging Computer Technologies
Research Article
Received: *2021-03-10* | ***Reviewing:*** *2021-03-11* & *2021-04-24* | ***Accepted:*** *2021-04-24* | ***Online:*** *2021-04-26* | ***Issue Date:*** *2021-12-31*

GoHammer Blockchain Performance Test Tool

Melih Birim
TUBU
İstanbul, Turkey
melih@tubu.io

Hüseyin Emre Arı
TUBU
İstanbul, Turkey
hemre@tubu.io

Enis Karaarslan
Department of Computer Enginnering
Muğla Sıtkı Koçman University
Muğla, Turkey
enis.karaarslan@mu.edu.tr

***Abstract*— Decentralized services are increasingly being developed and their Decentralized applications are increasingly developed but their performance metrics are not tested enough. The total number of transactions that can be supported by the blockchain network and the performance effects of selecting different consensus protocols, using different block intervals and block size should be tested. There are some blockchain performance tools but most are built for specific blockchain frameworks and require complex configuration. The GoHammer tool is developed to provide an easy to use, flexible test tool for the Ethereum/Quorum blockchain frameworks. Transaction per second (TPS) values and several performance metrics will be tested. This tool is also a part of the series of tools that can be integrated with Tubu-io. This tool will help in developing more efficient decentralized systems and will affect decreasing the costs of developing decentralized application projects.**

Keywords*— *Blockchain, smart contract, performance testing, stress testing, decentralized application

I. Introduction

Blockchain technology enables us to have trusted services without using an intermediary. Smart contracts that are introduced with Ethereum can be used to form autonomous Decentralized applications (DAPP) [1].

The availability and integrity of the blockchain systems increase with the number of nodes, but this also decreases the system performance [2]. However, performance tuning is possible by deploying different types of nodes and using different consensus protocols, using different block writing intervals or block sizes.

In the next section, performance evaluation in decentralized systems is explained. Related works are provided in the third section. The proposal of the system architecture and the implementation is explained in the fourth section. The results and conclusions are included in the final section.

II. Performance Evaluation

The sample test scenario can be used for the performance evaluation is shown in Fig 1. It consists of the blockchain network which will be tested and the test node. The system needs at least one test device which will generate the load and then observe the results, which will be called the TestNode in the document. The main performance metrics are as follows:

- Latency:
  - Read Latency
  - Transaction Latency
- Throughput:
  - Read Throughput
  - Transaction Throughput
- Resource utilization (CPU, Memory, Network IO, . . .)
- Number of failed/delayed transactions due to timeouts [7]

III. Related Works

There are several test tools for specific blockchain environments that are used to test decentralized applications (DAPP). Selected environments are compared in the Table 1. Currently, the most comprehensive performance benchmarking environment is the Hyperledger Caliper (https://hyperledger.github.io/caliper/). It supports many platforms other than Quorum. It can collect several performance metrics. Test transactions and scripts can be prepared for the use case scenarios. Sample implementations are given in [3-5, 7].

GoHammer tool is highly inspired by the Chainhammer (https://github.com/drandreaskrueger/chainhammer) and Consensys's Quorum Profiling [8]. We needed a test tool other than these two available tools as both are not easy to use and need complicated installation steps. Also Chainhammer's some required dependencies are outdated.

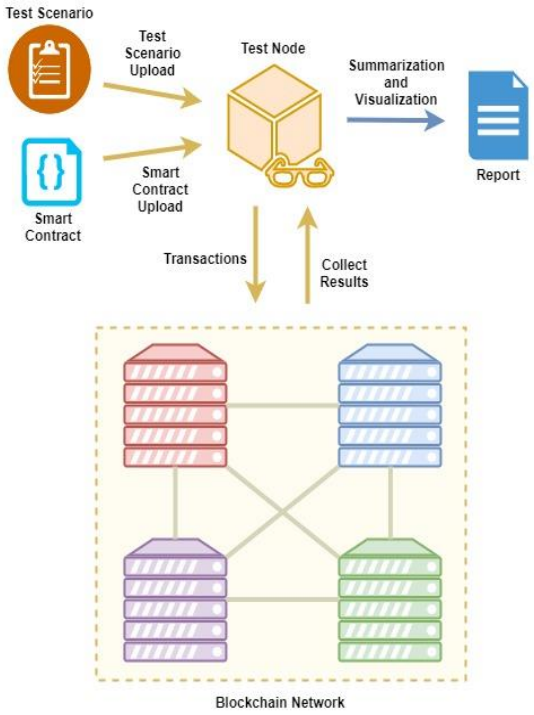

Fig. 1: Test Scenario

Cite (APA): Birim, M., Arı, H.E, & Karaarslan, E. (2021). GoHammer Blockchain Performance Test Tool. *Journal of Emerging Computer Technologies*, 1(2), 31-33.

Table 1. Comparison table

Product	*Caliper*	*Chainhammer*	*Quorum Profiling*	*GoHammer*
Platform	Hyperledger Besu, Ethereum, Hyperledger Fabric, FISCO BCOS	Quorum, Parity	Quorum	Quorum
Transaction/read throughput	Yes	Yes	Yes	Yes
Transaction/read latency	Yes	-[1]	No[1]	No
Resource consumption	Yes	No[1]	No	No
Consensus Protocol	-[1]	Raft, IBFT, Tobalaba	Raft, IBFT	Raft, IBFT[2]
Easy to Use	No	No	Partial	Yes
Minimal Installation [3]	No	No	Partial	Yes
Up to date	Yes	Partial	Partial	Yes
Programming Language	Javascript	Python	Golang	Golang

[1] Not clearly specified, [2] In the next Release, [3] Easy to install and less number of dependencies

IV. GoHammer Blockchain Performance Test System

GoHammer blockchain test tool generates transactions, runs test profiles and collects the TPS and resource consumption of the system. GoHammer is used with the TPS-Monitor components such as Grafana, InfluxDB and Telegraf. Telegraf is used to collect the data from the nodes. InfluxDB is used to store that data. Grafana is used to visualize the data. Docker is used for grafana and influxdb. The system architecture is shown in Fig 2.

GoHammer is developed using the golang programming language, especially for the Quorum blockchain framework. The test environment is formed of two main parts:

- Generating load on the system: Test profiles are managed and transactions are produced. The core GoHammer tool is used.
- Collecting and visualizing TPS and system metrics: TPS-Monitor (https://github.com/ConsenSys/quorumprofiling/tree/master/tps-monitor) that is taken from quorum-profiling toolset is used in this phase.

GoHammer parses the configuration file that contains information about the nodes involved and how the transactions will be produced. All transactions are produced on one node by default. If the scenario needs more than one Test Node, transactions will be produced with the round robin method. Consequent test profiles can be activated and each will have its own metrics and statistics. As an example; the first test scenario may have 1000 transactions and the second one 2000. The system will not generate any transaction for the given timeout value. Timeout values are set in human readable format like “1m”, “30s”, “10ms” etc. If you don’t want any timeout you can set this value to “0s”.

GoHammer has a compiled smart contract which can be used to produce transactions on the blockchain. The transactions can also be produced by calling this precompiled smart contract’s “setItem” method by setting “callContractMethod” field to true in the test config file. Currently resource consumption is only collected when this tool is run on a blockchain node. Collecting for different blockchain nodes will be possible in future releases when an agent is used.

Gohammer summarizes the results after the test scenario is finished. The log file is automatically named with the timestamp of the test date and time (DD_MM_YY mm:hh.log). The test execution time, test section execution time and the number of transactions produced is included in the log. Visualization processes are implemented with Grafana and sample screenshots of the implementation are given in Fig 3 and Fig 4.

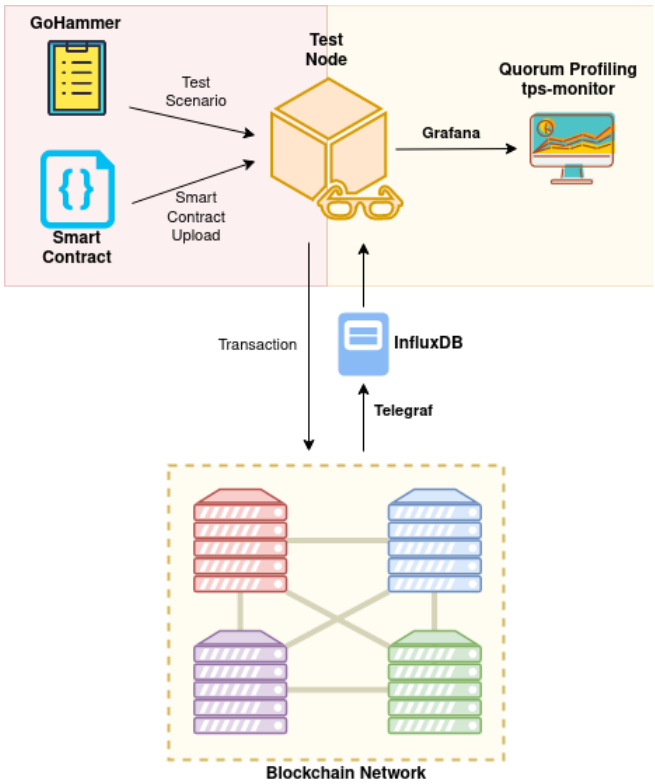

Fig. 2: Blockchain Test System Architecture

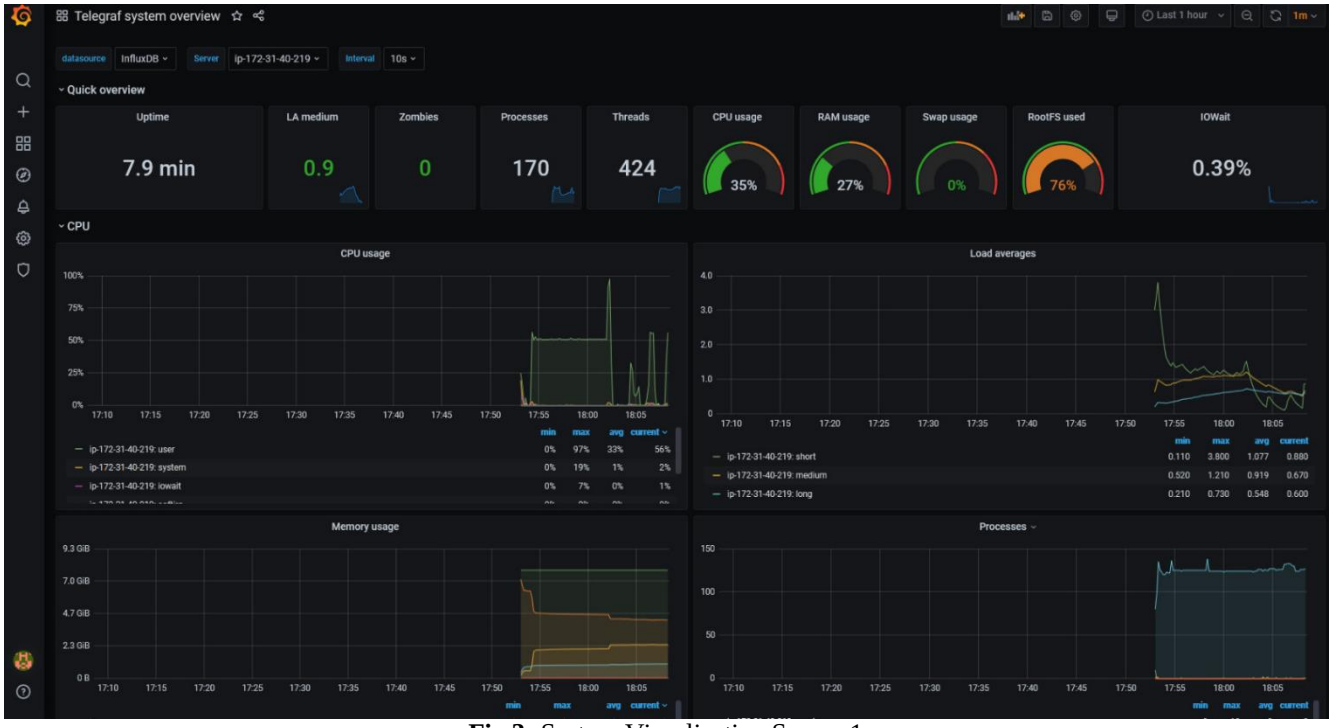

Fig.3: System Visualization Screen 1

Fig. 4: System Visualization Screen 2

V. Conclusion

We use GoHammer not only for research and academic projects but also in our commercial projects to test our decentralized applications performance. We are still working to improve it by opening its source codes with GPL licence on GitHub (https://github.com/tubuarge/gohammer).

It is planned to integrate with Tubu-io [9]. It will help in developing more efficient decentralized systems and is supposed to affect decreasing the costs of developing decentralized projects.

Acknowledgment

We would also like to thank Cemal Dak for his contribution in the graphics.

References

[1] Karaarslan, E. & Konacakli, E. (2020). Data Storage in the Decentralized World: Blockchain and Derivatives. In Gulsecen S., Sharma S., Akadal E.(Eds.), Who Runs The World: DATA (pp. 37-69). Istanbul, Istanbul University Press.

[2] Hyperledger Blockchain Performance Metrics (2018), Obtained from https://www.hyperledger.org/learn/publications/blockchainperformance-metrics

[3] Kuzlu, M., Pipattanasomporn, M., Gurses, L., Rahman, S. (2019, July). Performance analysis of a hyperledger fabric blockchain framework: throughput, latency and scalability. In 2019 IEEE international conference on blockchain (Blockchain) (pp. 536-540). IEEE.

[4] Pongnumkul, S., Siripanpornchana, C., Thajchayapong, S. (2017, July). Performance analysis of private blockchain platforms in varying workloads. In 2017 26th International Conference on Computer Communication and Networks (ICCCN) (pp. 1-6). IEEE.

[5] Nasir, Q., Qasse, I. A., Abu Talib, M., Nassif, A. B. (2018). Performance analysis of hyperledger fabric platforms. Security and Communication Networks, 2018.

[6] Hyperledger Getting Started, Obtained from https://hyperledger.github.io/caliper/v0.4.2/getting-started/

[7] Wickboldt, C. (2019). Benchmarking a blockchain-based certification storage system (No. 2019/5). Diskussionsbeiträge.

[8] Quorum Profiling (2021), Obtained from https://docs.goquorum.consensys.net/en/stable/Concepts/Profiling/

[9] Işık, E., Birim, M., Karaarslan, E. (2021). Tubu-io Decentralized Application Development Test Workbench. arXiv preprint arXiv:2103.11187.

Journal of Emerging Computer Technologies
Research Article
Received: *2021-02-09* | ***Reviewing:*** *2021-04-27* & *2021-05-20*| ***Accepted:*** *2021-05-21* | ***Online:*** *2021-05-21* | ***Issue Date:*** *2021-12-31*

Face Recognition Based Multifunction IoT Smart Mailbox

Radosveta Sokullu
Department of Electrical and Electronics Engineering, Ege University
İzmir, Turkey
radosveta.sokullu@ege.edu.tr

Özkan Akın
Department of Electrical and Electronics Engineering, Ege University
İzmir, Turkey
ozkan.akin@ege.edu.tr

Erginay Aslan
Department of Electrical and Electronics Engineering, Ege University
İzmir, Turkey
erginay-aslan@hotmail.com

***Abstract*— The abundance and variety of the Internet of Things (IoT) applications in the recent couple of years has reach a new record. From smart home, smart traffic, smart city, to industry, logistics and agriculture IoT applications are penetrating in every facet of our life and our society. A lot of simple and more complicated solutions benefit from the flexibility and diversity of connections that this new technology provides. In order to provide better management, better visualization, increase scale and reduce response times logistics and warehouse management are embracing new ways to improve upon the already "old" RFID technology. In this sense IoT provides an unprecedented technology to meet all these requirements in a uniform and easy to manage way. In this work a specific smart application – IoT mailbox with face recognition is discussed. Combining cellular connectivity with image processing it ensures the user that his valuable documents will be securely delivered. The developed prototype consists of a fingerprint reader, a camera, electromagnetic lock, a small LCD screen, a microphone and a loudspeaker all connected to an Arduino Uno which processes the data and establishes the network connectivity through a GSM module. Additionally, to perform face detection and recognition based on a prerecorded image set the camera is connected to Raspberry Pi and OpenCV and Python software is employed. The remotely controlled electromagnetic lock ensures that shipments are kept protected until the designated receiver takes possession of them.**

Keywords— IoT, Cellular Network, face detection, face recognition, electromagnetic lock component

I. INTRODUCTION

Logistics and transportation were one of the first sectors to embrace the RFID technology when it first appeared over a decade ago. [1] Requiring object identification and secure connectivity over large geographical areas and seeking to improve the supply chain solution upon RFID technology the transportation industry has already embraced IoT as a great tool to visualize location and manage critical goods in real time. The new IoT supply chain streamlines field operations, reduces inefficiencies and delivers better insights that improve client service levels. [2,3] Today, more than ever millions and billions of goods travel thousands of miles, changing hands many times or more, before they reach their final destinations. In this complex landscape, missteps along the supply chain are unavoidable. No matter how well established the logistics network is, at some point a truck will get stuck in traffic, or a packet will be delayed at a warehouse, or an asset will go missing altogether.

There is a lot of work related to solving these and similar problems especially using IoT. ADDSMART is a research project focused on digitizing addresses of locations and building a smart mailbox by combining wireless sensors, cameras, locks, and RFID readers and tags into a system controlled by an Arduino microcontroller board. [4] In [5] the authors describe the overall topology and prototype implementation of an intelligent mailbox using concepts of IoT to facilitate monitoring of physical mailbox installed at homes and offices. The system uses Nvidia Jetson TX1 controller and on board Wi-Fi module as preferred medium of communication between devices. Other hardware modules include secondary controllers which are Raspberry Pi 2B, RP2B Camera module with 5 megapixel fixed focus camera and TP-Link TL-WN722N wireless adapter for RP2B. Another interesting application is described in [6]. The authors propose a multi-functional parcel delivery locker (MFPDL) which utilizes C51 MCU and GSM/GPRS modules to send customers SMS with passwords in order to validate the acceptance of the shipment.

In this paper an example IoT application related to secure delivery of shipments and assets is described. "Smart Mailbox" addresses the secure and reliable delivery of mail and informs the user of the actions of the courier or logistic service. Different from other similar systems it uses several alternative methods (SMS, voice and face recognition) to realize the above mentioned functions and using off-the-shelf elements keeps the overall cost quite low. From here on the paper is organized as follows: in the next Section II the system architecture is presented, followed by details on the hardware components and software design in Section III. Section IV describes the experimental part and evaluates the results.

II. SYSTEM ARCHITECTURE

The proposed system aims to make one specific link of the logistics chain more secured. Usually when important documents and shipments are delivered the courier request a signature. However, to do this, the recipient has to wait at home and sometimes this might be quite inconvenient. The designed prototype allows the user to receive a document or shipment in a secured way irrelevant or whether he is at home or not. With the Smart Mailbox, the courier can leave the shipment in the mailbox only after it is remotely opened by the user and the user can retrieve the shipment at a convenient time only if he is cleared by the system as a legitimate user. When the courier arrives and tries to access the mailbox a notification is sent to the related user. Verifying that the shipment is the one he is expecting, he can remotely open the Smart Mailbox so that the courier can leave the shipment. Upon arriving home, the user's identity is checked against a predefined image set using face recognition and the mailbox

Cite (APA): Sokullu, R., Akin, Ö, & Aslan, E. (2021). Face Recognition Based Multifunction IoT Smart Mailbox. *Journal of Emerging Computer Technologies*, 1(2), 34-37.

is opened so he can retrieve his shipment. The architecture of the system realizing this functionality is given in Fig. 1.

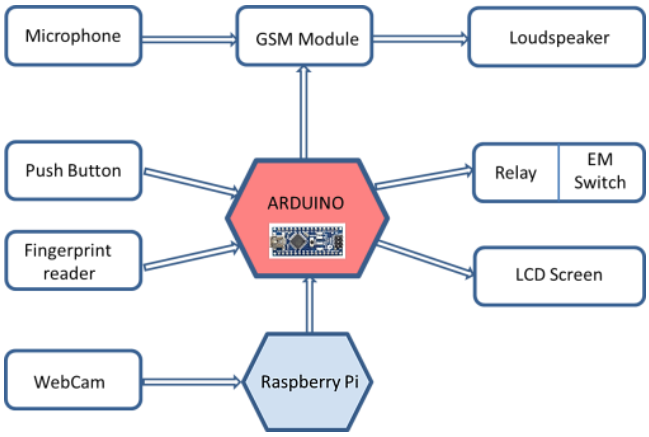

Fig. 1. General system architecture

Upon arrival the courier can contact the user either vocally by placing a call or sending an automatic sms by pressing one of the options ("Call" or "Send SMS") on the LCD screen of the mailbox. These functions are realized using the GSM module and related MIC and Loudspeaker blocks. The user checks the delivery and opens the lock by sending an opening code followed by a registered signature. The code activates the electromagnetic lock and the box is opened so the shipment can be placed inside. Upon arrival home the user is identified either by his fingerprint or by face recognition (fingerprint reader, camera and Raspberry Pi). The result activates the electromagnetic lock block and the mailbox is opened for the user to retrieve the shipment.

The above described elements are controlled by an Arduino Uno, while the face detection and recognition are realized using the OpenCV software running on the Raspberry Pi.

The initial LCD screen is as given on Fig. 2.

Fig. 2. Initial State of the LCD screen

Upon receiving a call or an SMS from a courier the user has two options: to accept and send a positive message "I accept" or reject by sending a negative message "I do not accept". These messages are received through the GSM module of the Smart Mailbox and interpreted based on the software designed. To increase security and privacy at the end of each message a special predefined signature code is added. In case the message is positive the software activates the relay and the switch is released; in case it is negative an additional notification is sent, shown on the LCD screen to inform the courier that the shipment is rejected.

If the mailbox opens the courier places the item and closes the door. It locks automatically and a message is sent to the user "Delivery accepted". At the same time, the information that the delivery is confirmed for the courier is sent to the screen of the mailbox.

The webcam controlled by the Raspberry Pi can also be kept active to check whether the person sending the sms is really a courier not just somebody who is tempering the mailbox. For this feature a continuous uninterrupted internet connection is required over cellular or wireless network, which turns it into a full scale real-time IoT application.

III. System Components

A. Hardware

The main hardware components used to realize the functionalities described above are: The Arduino Uno, the Mic and the loudspeaker, the fingerprint reader, the relay and the electromagnetic lock, the webcam and the Raspberry Pi.

The electromagnetic lock is an enameled copper wire with a diameter of 0.2 mm and length of 9 meters is wrapped around hollow cylinder with a length of 15 mm and 10 mm diameter. The core is temporarily magnetized when the coil is supplied with 5V 230 mA. To control this switch by the Arduino (max 45 mA) an additional relay is required.

The LCD screen used in the project is 5110 with 84X48 pixel resolution, DPI serial connection interface, working voltage 2.7V - 3.3V. An Arduino Pro Mini compatible fingerprint module which can store up to 1000 fingerprints was used. It supports fingerprint entry, image processing, fingerprint comparison and fingerprint search mode.

The brain of the system is the Arduino Uno with GSM shield. These hardware components are mounted together on the control panel at the front of the Smart Mailbox.

B. Software

There are two main components of the software designed for this prototype: the main operational algorithm and the face recognition related software.

The main algorithm is given below in Fig. 3.

The main algorithm controls 3 variables. These are send_message_button, call_button, and mail_compartment's reed switch information. If the courier clicks the send message button, the message with the shipment will be forwarded to the recipient and the "message has been forwarded please wait" information will be displayed. Remote receiver confirmation is required to open the mailbox. If the recipient types "open the box", the cargo_compartment function works which causes the electromagnetic lock to open. Information about the opening of the compartment is transmitted to the courier via display. After the courier leaves the shipment and closes the cover, both parties (the recipient and the courier) are informed.

If the courier has clicked the make call button, voice calls are made with the receiver via the speaker and microphone in the mailbox via the GSM module. After the interview is over, the process continues through the message receiving and decision functions.

If the postman leaves mail in the mail compartment, reed switch sends information to Arduino Uno and the recipient is informed by SMS.

If the Arduino Uno receives defined person Id information from the Arduino Pro connected to the fingerprint reader or Raspberry Pi connected to the camera, the cover is opened by running the cargo_compartment function.

```
Loop
Get send_message_button's information from left button
Get call_button's information from right button
Get mail_compartment's information from reed switch
If send_message_button is high
    Sms Print "You have shipment."
    Display "Message sent, please wait."
    Call take_a_message function
    Call decision function
Endif
If call_button is high
    Display "Call made, please wait."
    Call the box owner
    Display "Waiting for response."
    Call take_a_message function
    Call decision function
Endif
If mail_compartment is high
    Sms Print "You have mail."
    Display "Mail received, thanks."
Endif
If the identified ID comes from Raspberry Pi
or the identified ID comes from fingerprint reader
    Call cargo_compartment
Endif
If the unidentified identity comes from Raspberry Pi
    Sms Print "There is someone in front of your box."
    Sms Print "See from the camera, from address 192.168.0.107"
Endif
EndLoop
Function take_a_message
    If gsm module available for reading sms
      While gsm keeps sending sms
          Read sms as a character
          Save characters to sms buffer variable
      EndWhile
    Endif
EndFunction
Function decision
    If the message is "open the box"
      Call cargo_compartment
      Sms Print "Your box opened."
      Display "Cargo received."
    Else
      Sms Print "You indicated that the shipment is not yours."
      Display "The recipient refused the shipment."
EndFunction
Function cargo_compartment
    Set electromagnetic lock to high
    Display "Cargo compartment opened"
    If cargo compartment closed
        Set electromagnetic lock to low
        Display "Cargo compartment closed"
    Endif
EndFunction
```

Fig. 3. Main Algorithm

If unidentified contact information is received from Raspberry Pi, the owner of the box will be sent an SMS stating that there is a foreign person in front of the box and it is recommended to watch it from the specified internet address.

The face recognition algorithm in this study is based on the Haar Cascade Classification. [7] The face recognition algorithm compares a previously detected and registered source face with a new face and makes an identity decision based on the similarity. Using the already trained image database in OpenCV Phyton code is developed to define the limits for the recognition. Face recognition is done in real-time.Local Binary Pattern Histograms (LBPH) method is used because it is less susceptible to light compared to EigenFaces and FisherFaces. [8, 9] Comparison is pixel-based within given coordinates.

IV. Experimental Scenarios and Results

The finalized prototype, given in Fig. 4, was tested for all stages of the operational cycle.

Fig. 4. Final prototype

The accuracy of the fingerprint reader in the tests is 19 in 20 attempts. The remote operation was tested with "Send Message" and "Make Call" keys and the keys worked in all 20 attempts. There are no repercussions during the conversation. because the speaker and microphone were placed on different planes of the box. The display refresh rate is satisfactory. When the Mail compartment was opened, sms was sent to the recipient correctly every time in 20 attempts. In all trials, the cargo hatch was safely opened and locked. Information on whether the cargo is in the box was correctly provided in all 20 attempts.

Table 1. Success Results Table of 20 Experiments Performed Under Different Lighting Conditions and Face Conditions

Number Of Successful Results In Different Lighting Conditions (Lumen)			
20 experiments	***2200 lm***	***1600 lm***	***970 lm***
Pre-identified person	20	18	17
Unidentified person	0	0	0

Number Of Successful Results In Different Face States			
20 experiments	***Glasses***	***Beard***	***Face Mask***
Pre-identified person	18	16	5
Unidentified person	0	0	0

Another set of tests were performed to evaluate the face recognition process. Table 1 above summarises the conditions and correct result from 20 experiments. The facial recognition code is affected by different light and facial conditions. When the luminous flux fell, the number of successful attempts also

fell. In different facial conditions, the number of successful results decreases as the visible part of the face decreases. The code in the unidentified person has not been successful in any case.

A series of images and fingerprints of a specified user were initially recorded. Then the system was tested for recognizing the user, for establishing the cellular connection and for rejecting unknown users or people that temper the system. An example of an unknown user (unrecognized) is given in Fig 5. The legitimate user is "Erginay" (left) the unrecognized one is "Hatice" (right).

Fig. 5. Legitimate and non-legitimate user recognition test

V. CONCLUSION

In this paper we have focused on the use of IoT for logistics applications. An example of such an application called "Smart Mailbox" is described in detail. The design of the prototype including system architecture, hardware components and software is presented followed by experimental scenarios and results. The developed prototype is a good example of how simple off-the-shelf elements can be used to provide IoT functionality, increase the flexibility of logistics and supply services and ensure more reliable and safe experience for the user.

The advantage this prototype provides to The Courier is that it is unimportant whether the buyer is at home during cargo delivery. The advantage of the receiver is that he can remotely control the delivery. The prototype was tested for correct operation and the results of the tests are provided. Thanks to the facial recognition it is not possible for strangers or unauthorized people to open the box. Furthermore, the system allows tracking unauthorized attempts by saving the photographs of those who have not been identified.

REFERENCES

[1] S. N Shukla, T.A. Champaneria, "Survey of various data collection ways for smart transportation domain of smart city", 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), DOI: 10.1109/I-SMAC.2017.8058265, 2017

[2] L. Yaqiong, T. Lei, C. K. M. LEE and T. Xin, "IoT based Omni-Channel Logistics Service in Industry 4.0," 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Singapore, 2018, pp. 240-243.

[3] M. Glöckner, A. Ludwig and B. Franczyk, "A Reference Architecture for the Logistics Service Map: Structuring and Composing Logistics Services in Logistics Networks," 2016 IEEE International Conference on Computer and Information Technology (CIT), Nadi, 2016, pp. 644-651.

[4] J. R. Tew and L. Ray, "ADDSMART: Address digitization and smart mailbox with RFID technology," 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, 2016, pp. 1-6.

[5] A. Muhammad and N. ur Rehman, "Intelligent mailbox with centralized parallel processing," 2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Shanghai, 2016, pp. 255-259.

[6] S. Ze-hong and Z. Guang-yuan, "Multi-functional Parcel Delivery Locker system," 2015 International Conference on Computer and Computational Sciences (ICCCS), Noida, 2015, pp. 207-210.

[7] Y. Zhao, J. Gu, C. Liu, S. Han, Y. Gao and Q. Hu, "License Plate Location Based on Haar-Like Cascade Classifiers and Edges," 2010 Second WRI Global Congress on Intelligent Systems, Wuhan, 2010, pp. 102-105.

[8] Shiguang Shan, Bo Cao, Wen Gao and Debin Zhao, "Extended Fisherface for face recognition from a single example image per person," 2002 IEEE International Symposium on Circuits and Systems. Proceedings (Cat. No.02CH37353), Phoenix-Scottsdale, AZ, USA, 2002, pp. II-II.

[9] M. Johnson and A. Savakis, "Fast L1-eigenfaces for robust face recogntion," 2014 IEEE Western New York Image and Signal Processing Workshop (WNYISPW), Rochester, NY, 2014, pp. 1-5.

Journal of Emerging Computer Technologies
Research Article
Received: *2021-08-20* | ***Reviewing:*** *2021-08-23* & *2021-09-15*| ***Accepted:*** *2021-09-18* | ***Online:*** *2021-09-18* | ***Issue Date:*** *2021-12-31*

Development of An Efficient Tool to Convert Regular Expressions to NFA

Mustafa Batar
Department of Computer Engineering
Burdur Mehmet Akif Ersoy University
Burdur, Turkey
mbatar@cs.deu.edu.tr
0000-0002-8231-6628

Kökten Ulaş Birant
Department of Computer Engineering
Dokuz Eylül University
İzmir, Turkey
ulas@cs.deu.edu.tr
0000-0002-5107-6406

***Abstract*—In the computing theory, while the term "Language" specifies the string set, the term "Regular Expressions" means the notation that builds, creates and generates these languages. Also, the term "Regular Expressions" creates the characters that structure and compose, which refers to the given strings, in order to search patterns for sample matching. In this context, this article tries to show how to convert "Regular Expressions" that is made up of characters into Nondeterministic Finite Automata (NFA), which is a character matching and character searching tool, by giving related algorithms and methods with their explanations in detail. Moreover, in this study, a new and efficient tool has been designed and developed in order to convert regular expressions to NFA. By the contribution of this application, an original conversion tool will have been gained in the computation area for benefiting it. As a natural result of this, an original NFA modelling tool will have been placed in the literature.**

Keywords—Computing theory, regular expressions, NFA, modelling.

I. INTRODUCTION

Today, humanity is in the middle of the information age. However, this age encompasses an intellectual power rather than a physical one. For the past 25-30 years, information technology has played a very important role in the world. But what this power can do is not yet known to us. If looked at the 1950s, only some of the people kept diaries, but now; most people post everything from international political events to their pet's favorite toy on their personal pages online for all to see. But still, for some reason, people still hold on to the idea that the concept of computation: numbers or punctuation or something like that [1].

Although the concept of computation does not only belong to the numbers or punctuation marks, the meaning of this concept is still not clearly and unambiguously known. Almost every person in the world thinks that if a person is dealing with accounting, s/he accepts that s/he is doing calculations. However, many also have different opinions about whether the brain is a computer or something else. If the brain is a computer, it turns out that all the thoughts are computations and all computations are thoughts. It is also known that; the virtual world in computer games is a reflection of the real world that has emerged as a result of calculations. Thus, a dilemma arises as to whether the real universe is a computer. This dilemma is addressed the question into mind: "If the universe is a computation, then what is not computation?" [1].

About 100 years ago, most people in the world thought that computing was a mental operation involving numbers, and therefore it was believed that information counting could only be performed by humans. But today, it is thought by the vast majority that the computation can only be performed by machines. In Western culture, the thinking capacity of humans is considered as the most important factor that distinguishes humans from animals. Also in this culture, private thoughts and feelings are considered as the main factor for the formation of personal identity. For this reason, thought or thinking is believed to be necessary both for living together and for personal development. It is pointed out that changes in ideas about the meaning of the concept of computation also cause changes in thinking and ideas about humanity. This reflects the change in concepts such as culture, excitement, anxiety or virtual. Despite hundreds of known articles and researches about the concept of computation so far, what this concept exactly is still preserves and continues to be confidential and its mystery [1].

II. RELATED CONCEPTS

A. Automata Theory

The related theory is a developmental process that emerged to attract and distinguish people from a particular type of computer or a particular programming language. In automata theory, the emphasis is on the mathematical example of the concept of computation. In the theoretical sense; since it is easier to control and direct the machines mathematically, this theorem on automata creates a model, brings the computational mechanisms or machines to the simplest and plainest level, and reveals the bareness of these machines in order to demonstrate and also to prove the capacities of these machines [2].

The mathematical models are generally not suitable or not useful for solving practical programming problems. Real programming languages are better suited and more convenient for solving these problems. Although these programming languages are easy to use, it is rather difficult to evaluate them in a particular format. Theoretically, the main idea, that the relevant machines are designed from top to bottom to be made the simplest and mathematically operable, should definitely not to be forgotten [3].

B. DFA – Deterministic Finite Automata

The related automata is a finite state machine that accepts or rejects a certain number of strings, and in automata theory, determines a single computational or run-automation for each string input. The concept of "deterministic" means that the computation is unique and only one. When looked at the previous studies and researches in order to understand better

the concept of "Deterministic Finite Automata (DFA)", it is seen that "McCulloch" and "Pitts" were the first researchers to put forward a concept similar to finite automation in 1943 [4].

DFA is defined as an abstract concept related to mathematics, but since it is "specific", "deterministic" and "certain", it has a structure and feature that can be applied and used in both software and hardware for solving various problems. For example, by means of a DFA, a software application can be modeled that reveals whether the entered e-mail addresses are valid or not. It can also identify and reveal a regular set of languages that help to do lexical analysis and pattern matching. With the help of various algorithms, transformation from nondeterministic finite automata to deterministic finite automata can be performed, carried out, and implemented [5].

C. NFA – Nondeterministic Finite Automata

The relevant automata is a generalized version of the deterministic finite automata defined above – DFA. In nondeterministic finite automata, there may be zero, one, or more connections between each state. In this automaton, if there is more than one connection coming out of a situation, it means that the branch is divaricating, but if this branch does not have any valid connections, this branch disappears, that is, it dies [6].

If the given input character string reaches the acceptance state, the NFA accepts this character string set, but if it does not reach the acceptance state at all, it rejects that string set. In this automaton, a single accept condition is sufficient, but for a reject condition all branches have to reject the character input string. This mechanism, which is carried out, is called the modeling of the computational concept [7].

D. Regular Grammar

Related grammar defines regular languages, and also has a specific format. If a grammar has one of the following forms, that grammar is regular, but if it does not, that grammar is irregular (not regular) [8] as defined below:

$S \rightarrow \varepsilon \mid S \rightarrow w \mid S \rightarrow T \mid S \rightarrow wT$

w: is any terminating character in a regular expression that cannot be defined as a null character.

T: is any character that will not terminate a regular expression.

The most important aspect of establishing grammar is to have the knowledge and information underlying the language. It should not be assumed that a language will have only one grammar because more than one grammar structure of the same language can be created and installed. The following table – Table 1 – shows the grammar structure of various languages. In this table (Table 1), each regular language is represented with the contribution of regular expressions [8]:

TABLE I. REGULAR EXPRESSIONS AND REGULAR GRAMMAR

Regular expressions	Regular grammar
a*	$S \rightarrow \varepsilon \mid aS$
(a+b)*	$S \rightarrow \varepsilon \mid aS \mid bS$
a*b	$S \rightarrow b \mid aS$
(ab)*	$S \rightarrow \varepsilon \mid abS$
ba*	$S \rightarrow bA$ $A \rightarrow \varepsilon \mid aA$

E. Regular Language

It is a language with the alphabet "Σ", and as a concept, it has emerged as the constant repetition of the following features and characteristics [9]:

The empty set "Ø", which is an empty language, is also a regular language.

A single letter (character) belonging to the alphabet is also a regular language ("a" $\in \Sigma$).

If languages "A" and "B" are regular languages, then the set "AUB" (union operation), set "AoB" (concatenation operation), and set "A*" (star operation) are also regular languages.

F. Regular Operation – Union Operation

Union operation takes all the sequences of the regular languages "A" and "B", and combines these sequences into a new language [10].

AUB = {x | x Є A V x Є B}; A = {hot, cold} and B = {woman, man}; then AUB = {hot, cold, woman, man}

G. Regular Operation – Concatenation Operation

Concatenation operation connects the beginning of the string of the regular language "B" to the end of the string of the regular language "A" [10].

A o B = {xy | x Є A Λ y Є B}; A = {hot, cold} and B = {woman, man}; then AoB = {hotwoman, hotman, coldwoman, coldman}

H. Regular Operation – Star Operation

Star operation applies to a single regular language, and adds any number of strings of that language together to assemble them into a new regular language [10].

A* = {$x_1x_2\ldots x_k$ | k is positive integer Λ all x_i Є A}; A = {hot, cold}; then A* = {Ø, hot, cold, hothot, coldcold, hothothot, hotcoldhot,...}

İ. Regular Expressions

It is the sorted form of the characters that make up the search pattern, and used to make pattern matching with the given character strings. In regular expressions, each character either contains its own lexical meaning or is at the meta level and expresses a meaning other than itself. Also, regular expressions can easily reveal the textual meaning of the given sample pattern, and adhering to this meaning, can develop multiple examples that are exactly similar to this model. In addition, regular expressions plays an important role in designing automations for processing text files, creating and developing specified text formats, and receiving arbitrary string inputs [11].

The regular expressions processor reveals regular language information that is used to describe regular languages. There is a separate grammar and syntax for each regular language, and accordingly, a separate development system for each regular expression. Moreover, regular expressions operators compile the codes given to them, test the target character string, split it into smaller strings, and reveal whether that string belongs to the regular languages given to them. Furthermore, regular expressions have a very important place in the computational world because they create a common criterion in computation. For this reason, systems of regular expressions introduce basic and secondary

criteria for grammar and syntax. Also, regular expressions operators can be found and included in various search engines, some text editors, some search and replace word dialogs, as well as various scripted text compilers [12].

III. Related Algorithms and Methods

Under this title, 6 main algorithms and methods – McNaughton and Yamada's Algorithm, Glushkov's Method, Thompson's Algorithm, Berry and Sethi's Algorithm, Chang and Paige's Algorithm, and Antimirov's Method – that convert and transfer regular expressions to nondeterministic finite automata (NFA) in the field of automata theory have been tried to be explained in detail.

A. McNaughton and Yamada's Algorithm

This method is an algorithm that is used to extract state graphs from regular expressions and has a high applicability. While applying this algorithm, fewer states than "2^P+1" are generally needed and the working time of this method is at most "$\Theta(m|x|)$". ($m = \Omega(s^2)$ – the highest possible number of connections in the state graph. s: number of alphabetic characters in regular expressions. x: bit vector.) To understand this method better and more clearly, be useful to look at the example in the following [13].

Let "P = 1(00U01)*0". In this expression, there are six positions, respectively: 1_1, 0_1, 0_2, 0_3, 1_2, 0_4. If "P" is rewritten with its positions, it becomes "$1_1(0_1 0_2 U 0_3 1_2)^* 0_4$". $\{1_1\}$ is the starting state of "P" while $\{0_4\}$ is the ending state of "P". When creating the state graph, the first thing to do is to consider the initial state. Next, it is decided which state this initial state will combine with according to the given input: where to go in the "0" input character or where to go in the "1" input character. The initial state in this example goes to $\{1_1\}$ state at input "1" and Λ – empty – state at input "0". If a state falls into this empty state, the automation will never be able to get out of this state, which is why it is called a "dead state". Continuing, $\{1_1\}$ will be in the $\{0_1, 0_3, 0_4\}$ state when the input "0" comes in, and "dead state" when the input "1" comes in. $\{0_1, 0_3, 0_4\}$ becomes $\{0_2\}$ when "0" is input, $\{1_2\}$ when "1" is input. It goes to $\{0_1, 0_3, 0_4\}$ state when the input "0" comes to the $\{0_2\}$ state, and goes to the "dead state" when the input "1" comes. Also, state $\{1_2\}$ has the same properties as state $\{0_2\}$ in terms of inputs and destinations. The created nondeterministic finite automata (NFA) in the light of this information is demonstrated in Figure 1 [13] in the following.

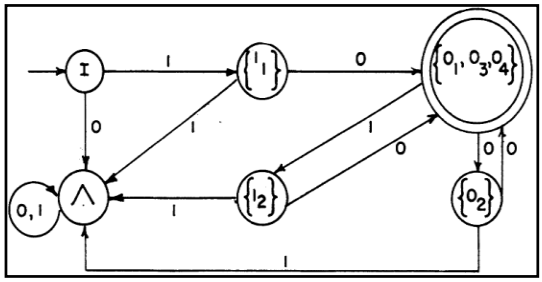

Fig. 1. NFA with McNaughton and Yamada's algorithm in the example.

B. Glushkov's Method

This method – also known as Glushkov's automation – transforms regular expressions to nondeterministic finite automata (NFA) using the subset construction algorithm. This algorithm creates a route path by matching the given string of characters with regular expressions with automation mechanism. It is decided how the states of this automation will be connected to each other with the help of this route. This algorithm uses a function on the nodes of regular expressions. With the contribution of this function, it reveals the empty and branching states in the automation, and thus all the necessary connection forms for a certain finite automata are revealed. Also, this method makes a complete transformation for NFA by including initial, acceptance and rejection states, and by eliminating redundant states in this automata [14].

C. Thompson's Algorithm

It is a method, also known as Thompson's configuration [15], which is among the algorithms that converts regular expressions to NFA. This algorithm breaks regular expressions into smaller regular expressions, and transforms these regular expressions into nondeterministic finite automata, and then combines these automata to produce the first given regular expressions translated into NFA. In addition, with this method, each character in the regular expressions is taken and tested in the order of their occurrence and transferred to the nondeterministic finite automata, thus avoiding the errors that may arise in the connections between the states and the route path. Also, this method starts parsing and splitting regular expressions from the left side and continues parsing and shredding in this way until the regular expressions are completed. In the Thompson's algorithm, the number of states is between "r-s()+1" and "2r", and the number of connections is between "r-s()" and "4r-3". (r: the length of the regular expressions. s(): number of parentheses in the regular expressions.) However, this method's runtime is up to maximum "O(r)" [15].

Based on the Thompson's algorithm, union operation is given in Figure 2, concatenation operation is demonstrated in Figure 3, and also star operation is shown in Figure 4 in the following.

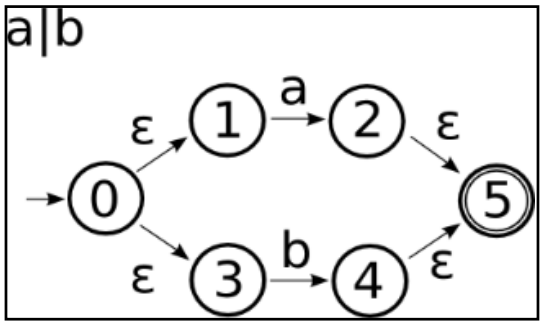

Fig. 2. Union operation based on Thompson's algorithm.

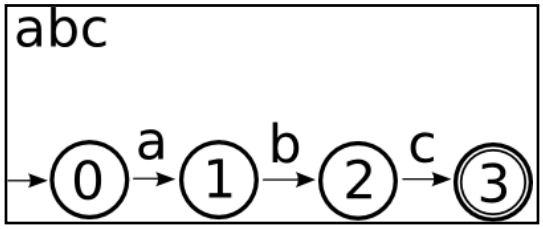

Fig. 3. Concatenation operation based on Thompson's algorithm.

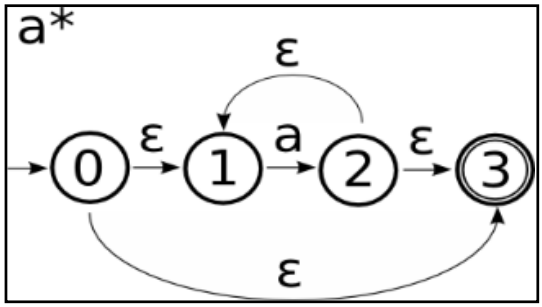

Fig. 4. Star operation based on Thompson's algorithm.

D. Berry and Sethi's Algorithm

This method is an algorithm that allows each symbol in regular expressions to appear in automation. The chart below (Figure 5 in the following) is an example of this algorithm, and reflects the regular expression "$(a_1b_2+b_3)^*b_4a_5$". In the automation built with this algorithm in the following figure (Figure 5), the "C" state has connections derived from the "C" state under certain and particular symbols and characters. While creating this automation, each link derived from each state is labeled with the same symbol. For this reason, all sequences of the automation derived from the "C_3" initial state have to also be in the "wb_3" format. Thus, it turns out that the automation of regular expressions derived from the initial state "C_3", and the automation of regular expressions derived from the initial state "C_0" are the same. In the Berry and Sethi's algorithm [16], the number of states in the nondeterministic finite automata (NFA) is maximum "s+1" and the working time of this algorithm is maximum "O(r)". (r: the length of the regular expressions. s: the number of alphabetic characters in the regular expressions.)

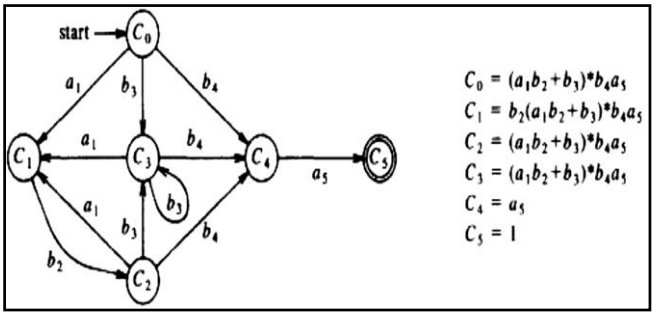

Fig. 5. NFA for the regular expression "$(a_1b_2+b_3)^*b_4a_5$".

E. Chang and Paige's Algorithm

This method generates the transformation from regular expressions to NFA in the same asymptotic time as with Berry and Sethi's algorithm – "Θ(m)". However, it is a method that has improved the auxiliary memory – the amount of "Θ(s)" – held in the memory of Berry and Sethi's method (s: the number of alphabetic characters in the regular expressions) [17].

The McNaughton and Yamada's algorithm lacks the number of connections between states in automation. Because if it is taken the worst case, the number of connections is "$m = \Theta(s^2)$". Also, if it is taken the expression "s()" as the number of parentheses (right or left), Thompson's nondeterministic finite automata (NFA) is the case between the numbers "r-s()+1" and "2r", as well as it has a connection between "r-s()" and "4r-3" (r is the length of the regular expressions.). For these reasons, a new compressed data structure has emerged – "Compressed Nondeterministic Finite Automata: CNNFA". This structure transfers regular expressions to a NFA occupying "Θ(r)" time and "O(s)" amount of memory [17].

F. Antimirov's Method

The corresponding algorithm converts a regular expression "t" into a nondeterministic finite automata (NFA) [18]. It uses the most "|t|+1" status while doing this operation. The details of this algorithm are explained in detail in the following.

In the given regular expression "t" according to the alphabet "A", let the automata be "M" and also, let the state sets be "M = PD(t)". The initial state is "$\mu_0 = t$", the coupling function is "$\tau(p,x) = \delta_x(p)$" – $p \in PD(t)$, $x \in A$ – and the end state sets are "$F = \{p \in PD(t) \mid o(p) = \lambda\}$". Accordingly, the "M" automata is be able to recognize the "L(t)" regular language. To put this construction structure into practice, the functions "PD(t)" and "τ" have to be calculated, and the following operations have to be repeated sequentially [18].

$$<PD_0, \Delta_0, \tau_0> := < \emptyset, \{t\}, \emptyset >$$

$$PD_{i+1} := PD_i \cup \Delta_i$$

$$\Delta_{i+1} := p \in \Delta_i \cup \{q \mid <x, q> \in \text{if } (p) \wedge q - \in PD_{i+1}\}$$

$$\tau_{i+1} := \tau_i \cup \{ <p, x, q> \mid p \in \Delta_i \wedge <x, q> \in \text{if}(p)\}$$

The working time of this algorithm is between "O(n)" and "$O(n^2)$" (n is the length of the given regular expressions.).

IV. Application – NFA Conversion Tool

A tool based on *Thompson Algorithm* [19-22] has been designed and developed in order to convert regular expressions to nondeterministic finite automata (NFA). This is a new and original application for modelling NFA according to given characters and expressions. NFA conversion tool works and performs based on the following directions.

With the arrival of the data, the NFA function starts to work. Each character in the regular expression is detected. These characters may be either a term or an action. Terms can be letters or numbers. Operations are union, concatenation and star operators. The union operation is given as the character "|", the concatenation operation is demonstared as the character "." and the star operation is also expressed with the character "*". When these characters are specified, it is understood that the terms will enter an operation. Also, the parentheses "(", ")" help determine the priority of the operations. According to the rules of these operations, it is determined that the terms, that are letters or numbers, go from which state to which state. When the NFA function completes running (finishes), all the states in the nondeterministic finite automata (NFA), and their trajectories appear exactly right. Thus, the necessary data for drawing the NFA are obtained.

Based on the application which have been designed and developed for modelling NFA, several regular expressions have been converted into nondeterministic finite automata in the study for showing its efficiency and usability: in Figure 6, the expression "a", in Figure 7, the expression "abc", in Figure 8, the expression "a*bc", and in Figure 9, the expression "(ab|bc)*" have separated, operated, transformed and drawn in the following.

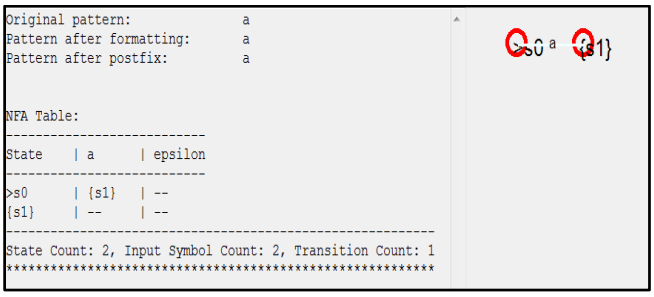

Fig. 6. NFA for the expression "a" in the developed tool in this study.

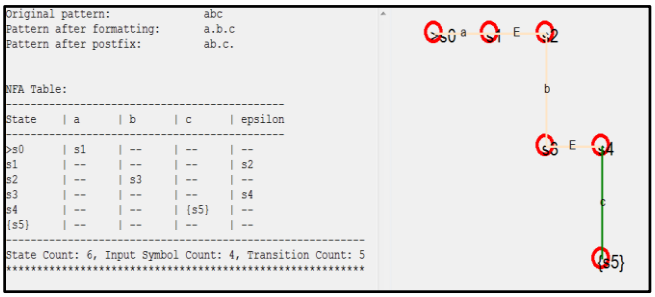

Fig. 7. NFA for the expression "abc" in the developed tool in this study.

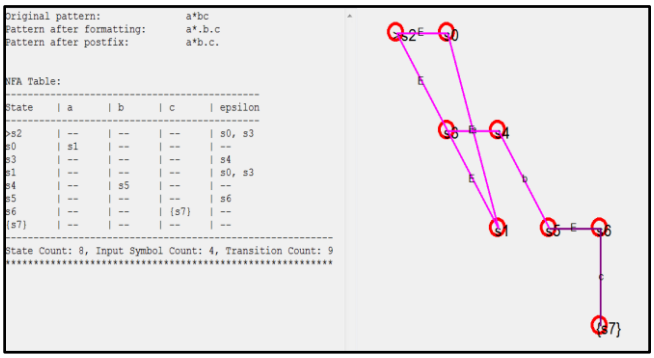

Fig. 8. NFA for the expression "a*bc" in the developed tool in this study.

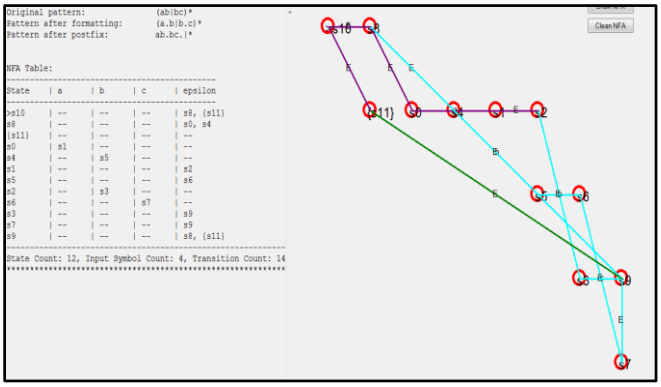

Fig. 9. NFA for the expression "(ab|bc)*" in the developed tool in this study.

V. Conclusion

Regular expressions are a representation in automata that make up regular languages. With the contribution of this notation, a given sample character string model can be tested; a text can be replaced with another; a smaller character string belonging to that string can be extracted from or added into a character string depending on the pattern match; word, text or symbol analysis can be performed. Also, regular expressions can be used effectively in search engines, natural language processing, parallel programming and neural networks. That means, regular expressions have an important role in computation area. With the help of this study, a tool has been designed and developed for that regular expressions are converted into nondeterministic finite automata (NFA). So, this tool may provide to understand more clearly and to benefit more effectively regular expressions for anyone who is interested in computing theory. In addition, this conversion application may be used in the studies and the researches about regular expressions. Thus, the tool, which have been designed and developed in this study, will have had a positive effect on both academic literature and computational industry.

Acknowledgment

Upon request, the executable file of the developed conversion tool and its source code within the scope of the study can be shared with the researchers who are interested in. Also, ethics committee approval form and document is not required for this study, and the authors declare that there is no conflict of interest.

References

[1] Horswill, I. (2008). What is computation? Obtained from https://users.cs.northwestern.edu/~ian/What%20is%20computation.pdf (Last access on 19th August 2021)

[2] Harvey, B. (1997). *Computer science logo style (1st ed.)*. USA: The MIT Press.

[3] Dlugosch, P., Brown, D., Glendending, P., Leventhal, M., & Noyes, H. (2014). An efficient and scalable semiconductor architecture for parallel automata processing. *IEEE Transactions on Parallel and Distributed Systems, 25*(12), 3088-3098.

[4] Lucas, S. M., & Reynolds, T. J. (2005). Learning deterministic finite automata with a smart state labeling evolutionary algorithm. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 27*(7), 1063-1074.

[5] Holzer, M., & König, B. (2004). On deterministic finite automata and syntactic monoid size. *Theoretical Computer Science, 327*(3), 319-347.

[6] Yang, L. Karim, R., Ganapathy, V., & Smith, R. (2011). Fast, memory-efficient regular expression matching with NFA-OBDDs. *Computer Networks, 55*(15), 3376-3393.

[7] Pao, D, Lam, N., & Cheung, R. A memory-based NFA regular expression match engine for signature-based intrusion detection. *Computer Communications, 36*(10-11), 1255-1267.

[8] Hopcroft E., Motwani, R., & Ullman, D. (2007). *Introduction to automata theory, languages, and computation (3rd ed.).* Britain: Pearson.

[9] Konstantinidis, S. (2007). Computing the edit distance of a regular language. *Information and Computation, 205*(9), 1307-1316.

[10] Owens, S., Reppy, J., & Turon, A. (2009). Regular-expression derivatives re-examined. *Journal of Functional Programming, 19*(2), 173-190.

[11] Lee, T. (2009). Hardware architecture for high-performance regular expression matching. *IEEE Transactions on Computers, 58*(7), 984-993.

[12] Kumar, S., Dharmapurikar, S., Yu, F., Crowley, P., & Turner, J. (2006). Algorithms to accelerate multiple regular expressions matching for deep packet inspection. *Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications,* 339-350.

[13] McNaughton, R., & Yamada, H. (1960). Regular expressions and state graphs for automata. *IRE Transactions on Electronic Computers, 9*(1), 39-47.

[14] Kurai, R., Yasuda, N., Arimura, H., Nagayama, S., & Minato, S. (2014). Fast regular expression matching based on dual Glushkov NFA. *Proceedings of PSC 2014,* 3-16.

[15] Thompson, K. (1968). Programming techniques: Regular expression search algorithm. *Communications of the ACM, 11*(6), 419-422.

[16] Berry, G., & Sethi, R. (1986). From regular expressions to deterministic automata. *Theoretical Computer Science, 48*(1), 117-126.

[17] Chang, C. (1992). *From regular expressions to DFA's using compressed NFA's.* PhD Thesis, New York University, New York.

[18] Antimirov, V. (1996). Partial derivatives of regular expressions and finite automaton constructions. *Theoretical Computer Science, 155*(2), 291-319.

[19] Brzozowski, J. A. (1964). Derivatives of regular expressions. *J. ACM 11*(4), 481-494.

[20] Kleene, S. C. (1956). *Representation of events in nerve nets and finite automata.* In Automata Studies, Ann. Math. Stud. No. 34. Princeton U. Press, Princeton, N. J., 3-41.

[21] IBM Corp. *IBM 7094 principles of operation.* File No. 7094-01, Form A22-6703-1.

[22] Kuno, S., & Oettinger, A. G. (1962). Multiple-path syntactic analyzer. Proc. *IFIP Congress,* Munich.

Journal of Emerging Computer Technologies
Research Article
Received: *2021-08-19* | ***Reviewing:*** *2021-08-19* & *2021-09-18* | ***Accepted:*** *2021-09-21* | ***Online:*** *2021-09-21* | ***Issue Date:*** *2021-12-31*

Coding Schemes in 5G Networks for Error-free Communication

Oliver Simonoski
UIST "St. Paul the Apostle"
Ohrid, Macedonia
oliver.simonoski@cse.uist.edu.mk
0000-0003-3623-6149

Ninoslav Marina
UIST "St. Paul the Apostle"
Ohrid, Macedonia
ninoslav.marina@gmail.com
0000-0003-4862-0199

Natasa Paunkoska (Dimoska)
UIST "St. Paul the Apostle"
Ohrid, Macedonia
natasa.paunkoska@uist.edu.mk
0000-0001-9639-2552

***Abstract*—The fifth-generation mobile communication network (5G) technology is a significant topic in today`s mobile communication industry. However, due to difficulties in the wireless channel generally, error-free communication is a big challenge. Thus, channel coding is a technology incorporated in the 5G mobile systems for achieving reliable and error-free two-way connections. In terms of data rate, capacity, coverage, latency, energy consumption, and cost, the fifth-generation (5G) communication systems must outperform previous fourth-generation (4G) systems. In this paper, we attempt to compare and evaluate the main characteristics of 5G channel and the performance of channel coding candidates. Low-density parity-check (LDPC) codes and polar are two capacity-achieving channel coding schemes that we concentrated on here. Block error rate (BLER), bit error rate (BER), computational complexity, and flexibility are all considered while analyzing the system. The results indicate that polar codes outperform the LDPC code systems, although LDPC is reasonable compared to other code systems.**

Keywords—5G, bit error rate, block error code, channel coding, LDPC code, polar code.

I. INTRODUCTION

The emergence of new technology demands and the need for the use of an increased number of various digital devices in our everyday lives brings the necessity to adopt new communication methods. High-speed computer-based systems allow practical and convenient work with advancements, and every year, leaders of the digital market introduce new networking and data transfer methods. The fifth-generation wireless connection, abbreviated as 5G, is one of these innovations. Previous generations have undeniable advantages; however, the new framework performs better and has more modern functionality. 5G intends to offer very high-speed connections, guarantee service quality, and serve mobile end-users as much as possible depicted in Fig. 1. The network behind this technology is wireless. This means there are unstable, unreliable and noiseless channels. To deal with the channel issue, a well-known technology channel coding is introduced. The study of efficient coding techniques is still ongoing and represent an open problem. Many different coding schemes today are present and already in use within the new technology networks. By incorporating them in the 5G network generally, this technology can provide considerable benefits in terms of increased capacity and coverage areas, data rates, dependability, availability, and low latency rates.

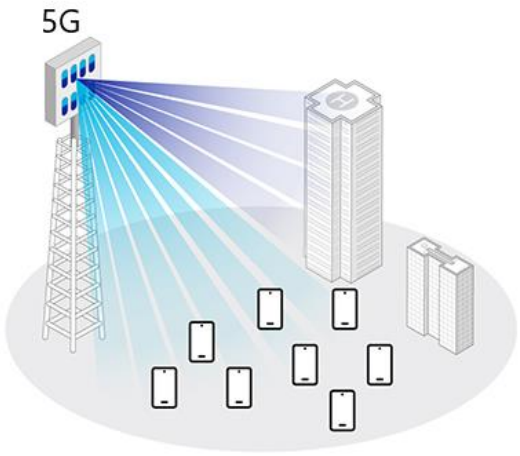

Fig. 1. 5G Networking

This paper will use two different coding schemes for analyzing the channel performance in 5G, a Low-Density Parity Check (LDPC) and Polar code. The Polar code schemes that we simulated in this work is a Polar code with consecutive cancellation decoding and successive cancellation list decoding. The LDPC code scheme is tested for two different parity-check matrices. The simulations are done by matching the parameters and characteristics of a 5G environment.

The rest of the paper is organized as follow: Section II gives the description of the related concepts and briefly gives the description of the 5G. Section III provides the characteristics of the coding schemes. Section IV presents the simulation stage and the preparation and modulation in terms of frame error rate (FER) and bit error rate (BER). The results from their comparison are presented in Section V and Section VI conclude this article.

II. RELATED CONCEPTS

5G wireless technology is meant to deliver higher multi-Gbps peak data speeds, ultra-low latency, more reliability, massive network capacity, increased availability, and a more uniform user experience to more users. Higher performance and improved efficiency empower new user experiences and connect new industries. For proper functioning 5G systems incorporate different access technologies into a single, seamless experience. The convergence and interoperability of terrestrial and satellite communication systems is one significant trend. Reference [1] considers the cognitive approach using an Adaptive Coding and Modulation protocol for the second user to ensure entering in a primary user frequency band. The assumption here is that the cognitive

receiver will need to recognize the start of the frame together with the code rate recognition point. Wireless caching technology also gaining popularity in 5G, especially in ultra-dense networks where many devices try to access different network services while being restricted by latency, energy efficiency, and bandwidth. The cache efficiency increases by using the concept of femtocaching, and addressing for file allocation [2]. Another way to guarantee a functional 5G network is to have successful New Radio Access Technology (NRAT). NRAT aims to examine the user channels and apply appropriate coding schemes to fit the wide range and diverse applications. According to the European research centre [3] when focusing on short message length ($k < 512$), the most appropriate coding schemes that are considered are Turbo, Polar, binary and non-binary LDPC and tail-biting convolutional codes.

One popular coding scheme intended for 5G is the Polar code [4], which provides excellent error-correcting efficiency. The turbo code was chosen as the primary channel code schemes in the previous network standards (3G and 4G). Still, the experience showed that this would not be the case in the 5G due to bandwidth and energy usage, latency, and complexity limitations. This conclusion comes from the simulation performed by Maunder er al. in [5], [6], and it can be concluded that they need to be replaced by (LDPC) code because of the benefits which are coming in the down-link, ultra-low latency, wide range, Internet of Things (IoT) and cloud computing. Focusing on block error results performed in the physical layer reference [7] showed that Turbo, LDPC, and polar codes give promising results on a wide range of coding rates and code lengths. Specifically, LDPC works fine even without using the CRC (Cyclic redundancy check), and the Polar codes do not have an error flow, but the code construction needs to be based on the channel, so they are not yet flexible. The major drawback of polar codes compared the LDPC codes is the increasing complexity and functionality and the dependence on the parity check matrix design [8]. Paper [9] demonstrated that the output from those codes is highly dependent on the duration of the related input and that larger block lengths (132 bits) need fewer repetitions of the code. When the coding length is 1024, the performance of LDPC and turbo codes are similar to each other, with the turbo code having an advantage at lower coding speeds [10], [11].

Another topic that needs to be mentions is the sub-layer for mobile video Streaming/Downloading in the cellular network, which is implemented to ensure secure and good video transmission. According to the previous work [12] perfect candidate is Random Linear Network Coding, which provides flexible input source blocks, source block length, source/encoded packet length, coding coefficient field size and many generated numbers of encoded packets.

There are many challenges regarding lower latency implementation, such as reliability, higher bandwidth, high spectrum efficiency, higher data rate. But the main focus stays on acquiring reliability and security simultaneously, as elaborated in [13]. Replacing of convolutional and Turbo codes with polar and low-density parity-check (LDPC) is done in 5G. Compared with polar codes, LDPC codes are part of the QC-LDPC code family, which can be explained using the protograph code principle. Protograph codes can be represented as a graph by adding several copies of the protograph and then permuting edges across them. Lifting is the method of adding several copies of the protograph and permuting their edges given in [14]. This method found wide commercial adoption and is represented with IEEE 802.11 standards. The reinforcement of this framework is the Q-learning algorithm [15], which enables the base station to choose suitable modulation and coding schemes that will maximize spectral efficiency while keeping a low block error rate. The previous works [16], [17] have assessed three different incarnations of successive cancellation list decoders for polar codes with different trade-offs between performance, latency, and complexity using the Extrinsic Information (EXIT) chart tool that evaluates the output of near limit channel codes. The results would help in the selection of a channel code for 5G and higher systems.

III. Underlying Theories

This section gives a brief description of both coding schemes, Polar and LDPC. Channel coding has been the transmission chain's first processing block, dedicating error correction and detection capability to the transmitted signal. Convolutional, turbo, LDPC and polar codes are among the four coding schemes supported by the model. Due to their outstanding performance and low complexity assert implementation, 3GPP (3rd Generation Partnership Project) chose these schemes as contenders for 5G. The previous standard follows the turbo and convolutional codes, but for the 5G new radio (NR) standards, we introduce the LDPC code. The LDPC decoder includes a layered design that incorporates the column message-passing schedule. In terms of decoding iterations, this provides for quicker convergence. The decoder for polar codes is based on log-domain successive cancellation (SC) and its extensions List-SC and CRC-aided List-SC.

The parameters of the codes are given in Table I, and then the encoding and decoding processes are elaborated, which later are used in the simulation program.

A. Polar code

Polar codes in detail are introduced in [11]. In general polar coding represents a channel polarization method where the channel is polarized into N channels (bit channels) that together with the duration of the codeword ($N \rightarrow \infty$) forms a new efficient channel that is entirely noise or noiseless. In these coding schemes, the number of bit channels is restricted. Thus, based on the code rate $R = \frac{K}{N}$ a good channel K from N channel in terms of bit error rate must be chosen. Polar code creation is the process of selecting a bit channel (W).

B. LPPC code

Gallager discovers LDPC code explained in [17]. Those codes for the encoding process use the concept of a sparse parity-check matrix H following the condition where the number of "1" bits need to be less than the number of bits of "0". All of this is represented using the Tanner graph, which is mainly a matrix divided into parts (bits nodes and check nodes).

C. Encoding Scheme of Polar Code and LDPC code

The LDPC code coding scheme used in this paper starts with creating the matrix H using Mackay random construction [12], permutation matrix H using the min-prod technique, encoding using the triangular factorization process, and decoding using the message passing algorithm (MPA) and the min-sum product algorithm (SPA) [14].

This paper`s Polar code encoding scheme starts with code construction using the Bhattacharya algorithm [4] to locate frozen bits. Then, the encoding and decoding of the Polar code is done by using successive cancellation (SC) and successive cancellation list (SCL) [2].

D. Decoding Scheme of Polar Code with Successive Cancellation (SC) and Successive Cancellation List (SCL)

The Successive cancellation (SC) decoder process, which can be represented as a binary tree search, starts with providing the codeword bit with a remark on channel output and using the previous codeword bit. On the other side, with the Successive cancellation list (SCL), we are using the list parameter to encode a codeword by seeing his decoding directory [8]. The algorithm estimates a bit considering both its possible values 0 and 1.

Parameters	***Specifications***
nbRM	Total number of codeword bits generated
K	Number of message bits
nL	List size
FER	Frame error rate
BER	Bit error rate
BLER	Block error rate
Nblkerrs	Number of block errors
Nbiterrs	Number of bit errors
Nblocks	Number of blocks

TABLE I. PARAMETERS AND SPECIFICATIONS OF CHANNEL CODING FOR SIMULATION SCENARIO

IV. SIMULATION

Simulations of the LDPC and Polar code encoding schemes are done to be determined the output in terms of block error rate (BLER) and frame error rate (FER). The simulation conditions, as well as the scenario predictions, are represented separately.

Step 1: Preparation stage or Setup and Code Construction Starting with the polar code, we set the parameters: the block length *n=1024, rate* $=\frac{1}{2}$. Next, we choose the SC decoding where *k=512*, but if we choose the SC list, we must specify the length of the message *l=500* and specify the CRC *length =11*. Now for the LDPC we have two options (base graph 1 and base graph 2). If we have the first case Base graph 1 then *k=22z* and *rate* $=\frac{1}{2}$ and the *codeword bit transmitted = 44z.* The variable *z* represents the expansion factor. According to Base graph 1 we have parity check matrix (46 × 68) where the first 22 rows are reserved for the message, then the remanding 46 are parity. So, for the proposed rate, showed in Fig. 2, we need to take 24 parity (from the parity part) because later those are used for the decoding part. Next thing we take the block length, but because we have fixed value for the *z* this will have base matrix 24. The process is similar for Base graph 2 in Fig. 3, but here the length of the parity check matrix is (42 × 52), so *k=10z*, codeword *transmitted = 20z* (and from here $z \approx 50$).

Step 2: Preprocessing Stage There is preprocessing stage before the bits of information are transmitted. That stage in LDPC is the construction and permutation of matrix *H*, whereas the phase in polar code is done only construction. The wight of the column is essential if matrix formation is of dimension $M \times N$. Next, matrix *H* is examined to avoid the occurrence of length cycles, which would result in increasing the decoding difficulty. Then, the permutation of matrix *H = [H1 | H2]* seeks to turn the matrix *H1* into a non-singular matrix. The Polar code is prepared using the SNR 0 design and the Bhattacharya algorithm in successive cancellation decoding. The Polar code creation algorithm is also utilized in successive cancellation list decoding, but with a value of $\varepsilon = 0.32$.

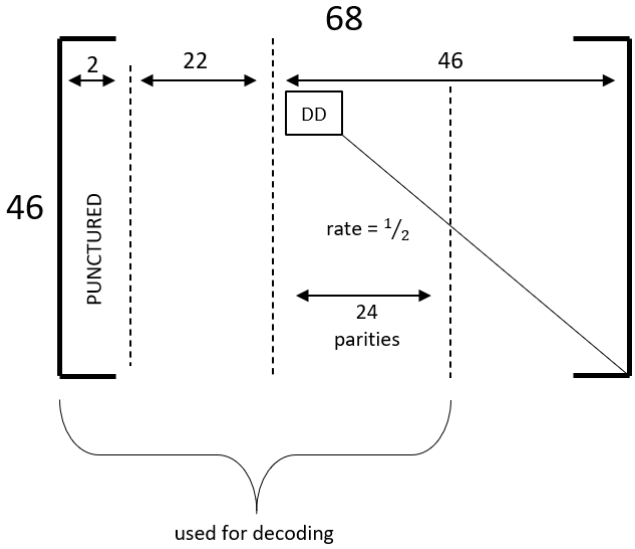

Fig. 2. LDPC, Basegraph1 – parity chech matrix

Step 3: Modulation Stage

Before we proceed to the next part, first, we must provide enough errors. After that, in the end, we are printing and putting in one matrix the results from frame error rate and bit error rate simulations, number of block errors, number of bit errors, number of blocks. In order to choose which data needs to be taken, we must perform this stage multiple times by reducing the numbers of the blocks until we get some errors, and then slowly to start with increasing. Last, we must provide the plotting details where *x* axis will keep the *log y* in liner scale and then *y* axis to semi *log y*.

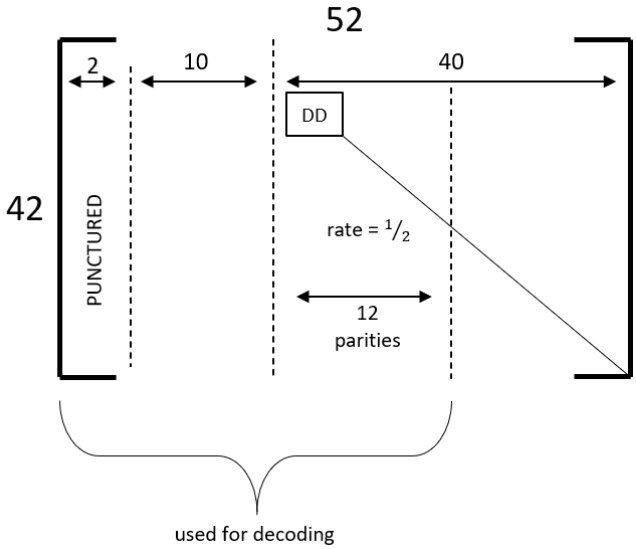

Fig. 3. LDPC, Basegraph2 – parity chech matrix

V. Performance Comparison

This section elaborates the performance among both codes, Polar and LDPC. The comparison is made regarding the coding rate and the number of bit or block errors during the data transmission time. Under all examinations, four different codes are considered: Polar code with successive cancellation, Polar code with successive cancellation list, LDPC based on Basegraph 1 and LDPC based on Basegraph 2. Fig. 4 calculates the achievable bit error rate of each code construction. The figure depicts that the polar code with successive cancellation decoder is the poorest one. As it is noticeable is located on the right side where for *3dB*, the value for FER goes to 10^{-3}. On the other side, the polar code with successive cancellation list decoding gives the best result, i.e., for 10^{-3} FER we get $dB \approx 2.1$. With the list size increasing to eight, the curves go more to the left and give good results. The LDPC with Base graph 1 and Base graph 2 are relatively equivalent with same size of block length, although we must consider the choice of parameters i.e., the quantization. In general, we can see that the polar code and the LDPC code are quite effective at these comparable block lengths, and they perform pretty well when quantized and simulated.

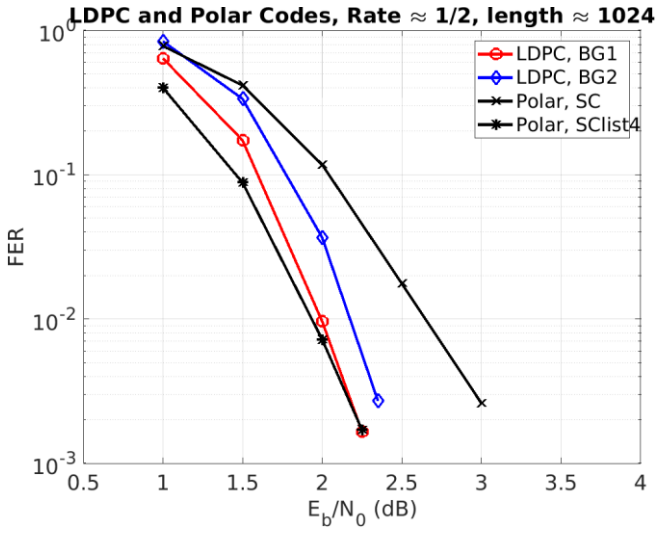

Fig. 4. LDPC and Polar Codes, Rate ≈ ½ , length ≈ 1024

Fig. 5 shows the number of bit errors compared to the value of the number of blocks. From the graphs can be understood that they all have similar results at the beginning of the x-axis, which in some way they perform close to each other, especially at the higher number of blocks. As expected, the polar code with SC gives the most bit errors at the beginning for smaller values. However, as the number of blocks increases, the Polar successive cancellation code outperforms the other ones. Still, it has the most significant value for errors, which is not the case with others. At the end of the x-axis, the improvement of the Polar with SC is slightly increased, and all other gives a constant increase.

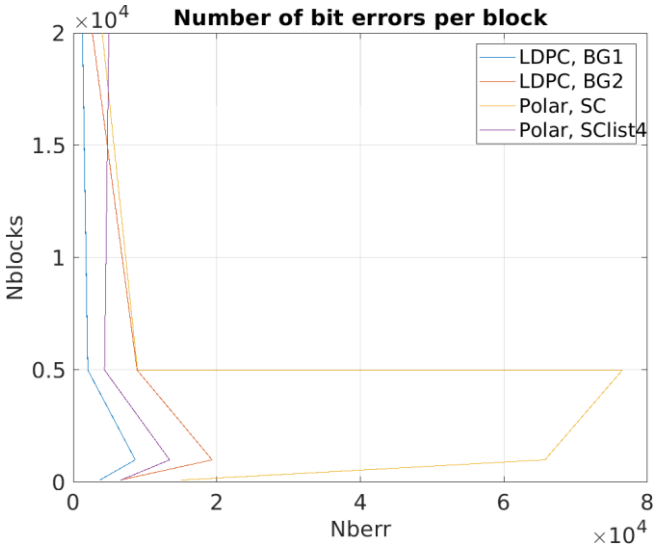

Fig. 5. Number of bit errors vs block

Fig. 6 compares the number of block errors vs the number of blocks. As shown in Fig. 6, it can be examined that in the situation where the number of blocks is greater than 1×10^4, the result is similar to each other for most of the coding schemes. They perform well, but it must be mention that the best performance gives the Polar with successive cancellation with list=4 where it meets the lowest parameters for the number of blocks errors compared to the number of blocks. On the other side, when the value for the number of blocks is below 1×10^4, the worst performance is given by Polar with SC which provides around 600 block error just for 0.5×10^4 blocks.

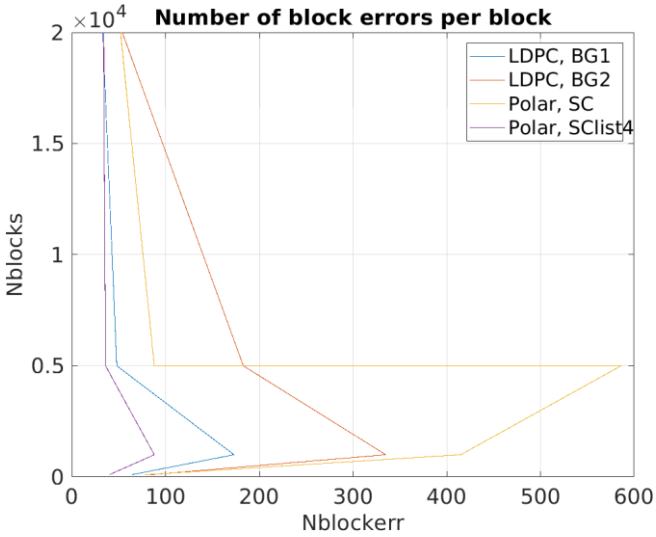

Fig. 6. Number of block errors vs block

VI. Conclusion

This work compares and estimates the efficiency of the Polar and LDPC codes as candidates for coding in the 5G networks. To different codes and four variations of them are considered in the simulations, the polar code with successive cancellation (SC), the polar code with successive cancellation list (SCL) decoding, LDPC code Base graph 1 and LDPC code Base graph 2 decoding. All coding schemes have a uniquely critical role in providing high throughput and low latency. To increase the value of block length, we must

decrease the $\frac{E_b}{N_o}$, and by this, we have a demand for less power consumption. Although the successive cancellation decoder for polar codes has the lowest complexity, the CRC-assisted successive cancellation list decoder outperforms LDPC and turbo codes. Due to a lack of implementations, the actual costs of these types of decoders are unknown. Many other considerations must be addressed when choosing a coding scheme, such as encoding and decoding delay, energy efficiency, and space efficiency. The polar code with successive cancellation list has the best performance with *2dB* related to other schemes in order to achieve FER 10^{-3}. In conclusion, polar codes with SCL become the best candidate as an effective encoding scheme for this concrete situation.

REFERENCES

[1] Tsakmalis, A., Chatzinotas, S., and Ottersten, B. (2014). ”Modulation and Coding Classification for Adaptive Power Control in 5G Cognitive Communications. 2014 IEEE 15Th International Workshop On Signal Processing Advances In Wireless Communications (SPAWC).” doi: 10.1109/spawc.2014.6941505

[2] Abdulwhab, W., and Kadhim, A. (2018). ”Comparative Study of Channel Coding Schemes for 5G. Journal Of Electronic Systems,” 8(3), 95. doi: 10.6025/jes/2018/8/3/95-102

[3] Iscan, O., Lentner, D., and Xu, W. (2016). ”A Comparison of Channel Coding Schemes for 5G Short Message Transmission. 2016 IEEE Globe-com Workshops (GC Wkshps).” doi: 10.1109/glocomw.2016.7848804

[4] Kim, H. (2015). ”Coding and modulation techniques for high spectral efficiency transmission in 5G and satcom. 2015 23Rd European Signal Processing Conference (EUSIPCO).” doi: 10.1109/eu-sipco.2015.7362884

[5] Maunder, R. (2016). ”A Vision for 5G Channel Coding.” Accelercomm White Paper.

[6] Fadlallah, Y., Tulino, A., Barone, D., Vettigli, G., Llorca, J., and Gorce, J. (2017). ”Coding for Caching in 5G Networks. IEEE Communications Magazine,” 55(2), 106-113. doi: 10.1109/mcom.2017.1600449cm

[7] Gamage, H., Rajatheva, N., and Latva-aho, M. (2017). ”Channel coding for enhanced mobile broadband communication in 5G systems. 2017 European Conference On Networks And Communications (Eucnc).” doi: 10.1109/eucnc.2017.7980697

[8] Kaykac Egilmez, Z., Xiang, L., Maunder, R., and Hanzo, L. (2020). ”The Development, Operation and Performance of the 5G Polar Codes. IEEE Communications Surveys & Tutorials”, 22(1), 96-122. doi: 10.1109/comst.2019.2960746

[9] Ligurgo, M. (2017). ”IoT for 5G: candidate coding schemes.” TORINO: POLITECNICO DI TORINO.

[10] Do-Duy, T., and Vazquez Castro, M. (2018).” Design of network coding functionality for 5G networks”. Barcelona.

[11] Sharma, A., and Salim, M. (2018). ”On The Feasibility of Polar Code as Channel Code Candidate for the 5G-IoT Scenarios. International Journal Of Future Generation Communication And Networking ” 11(3), 11-20. doi: 10.14257/ijfgcn.2018.11.3.02

[12] Vukobratovic, D., Tassi, A., Delic, S., and Khirallah, C. (2018). ”Random Linear Network Coding for 5G Mobile Video Delivery. Information,” 9(4), 72. doi: 10.3390/info9040072

[13] Arora, K., Singh, J., and Randhawa, Y. (2019). ”A survey on channel coding techniques for 5G wireless networks. Telecommunication Systems,” 73(4), 637-663. doi: 10.1007/s11235-019 00630-3

[14] Bae, J., Abotabl, A., Lin, H., Song, K., and Lee, J. (2019). ”An overview of channel coding for 5G NR cellular communications. APSIPA Transactions On Signal And Information Processing,” 8. doi: 10.1017/atsip.2019.10

[15] Mota, M., Araujo, D., Costa Neto, F., de Almeida, A., and Cavalcanti, F. (2019). ”Adaptive Modulation and Coding Based on Reinforcement Learning for 5G Networks. 2019 IEEE Globecom Workshops (GC Wkshps).” doi: 10.1109/gcwkshps45667.2019.9024384

[16] Pillet, C., Bioglio, V., and Condo, C. (2020). ”On List Decoding of 5G-NR Polar Codes. 2020 IEEE Wireless Communications And Networking Conference (WCNC).” doi: 10.1109/wcnc45663.2020.9120686

[17] Shah, P., Vyavahare, P., and Jain, A. (2020). ”Performance Evolution of Modern Error Controlling Codes for future generation (5G) cellular systems: LDPC code.” doi: 10.21203/rs.3.rs-22526/v1

Journal of Emerging Computer Technologies
Research Article
Received: *2021-08-19* | ***Reviewing:*** *2021-08-19* & *2021-09-18* | ***Accepted:*** *2021-09-21* | ***Online:*** *2021-09-21* | ***Issue Date:*** *2021-12-31*

Coding Schemes for DNA Patient Record Processing to Electronic Health Records Systems

Izabela Mitreska
UIST "St. Paul the Apostle"
Ohrid, Republic of North Macedonia
izabela.mitreska@cse.uist.edu.mk
0000-0002-0848-9416

Ninoslav Marina
UIST "St. Paul the Apostle"
Ohrid, Republic of North Macedonia
ninoslav.marina@gmail.com
0000-0003-4862-0199

Natasa Paunkoska (Dimoska)
UIST "St. Paul the Apostle"
Ohrid, Republic of North Macedonia
natasa.paunkoska@uist.edu.mk
0000-0001-9639-2552

***Abstract*—Lately, electronic health record (EHR) systems became very popular in medical technology. The main aim of such systems is to perform a digital version of a patient's paper chart. EHRs are real-time, patient-centered records that make information available instantly to authorized users. One critical patient record is the DNA sequence, which should be processed and stored in the EHR without any modifications. Therefore, in this paper, we focus on how DNA sequence can be reliably processed to EHR systems. By introducing coding technique on top of the information we implemented the wanted security. We consider and analyze two coding schemes, the Hamming code and Reed-Solomon, on the same data sample. The results are summarized and compared by error detection and error correction values. The final outputs show that Reed-Solomon coding scheme outperforms the Hamming code scheme for reliably and securely processing the DNA record to the EHR.**

Keywords— Electronic Health Records, encoding, decoding, Hamming code, Reed-Solomon code.

I. INTRODUCTION

The constant emergence of new technologies on a global scale introduced the digitalization of healthcare services by implementing different Electronic Health Records (EHR) systems. EHR systems are electronic versions of patients' medical and treatment card history that improve health surveillance and clinical decision making. The availability of complete medical information allows physicians to distinguish chronically ill patients and identify the proper diagnose intended to provide medical treatment. Early intervention of health-related issues is fundamental for the effective treatment and avoidance of further medical complications. Mitreska et al. state in [1] that by granting adequate diagnoses and treatments, medical personnel gain the opportunity to safeguard people's lives in an effective and timely manner.

Nowadays there is a common implementation practice of EHR systems in patient's data management as shown in Fig. 1, i.e. introducing health tracking, diagnoses, different applied therapies, physicians' reports, information for deoxyribonucleic acid (DNA), etc., to improve the healthcare process. Hence, this type of system can be applied to create flexible architectures that facilitate healthcare structure interoperability. The main characteristics of EHR systems are proprietary data flow formats and encoding schemes, which hinder the possibility of sharing data in a standard format. For example, data from a hospital that offers cancer treatments, which is a source for further data processing in this situation, should be extracted and mapped to the EHR system of other department or hospital that offer different service as depicted in Fig 2. This means that in order to realize successful general implementation, a special emphasis must be put on the sensitive data transfer path or the information processing among the diverse entities.

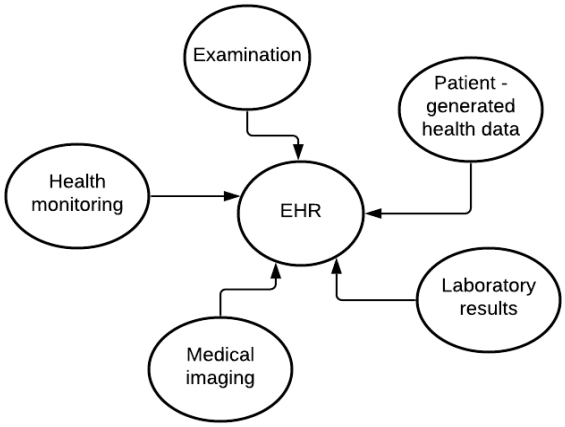

Fig 1. EHR systems

Therefore, this paper chose one sensitive patient information, a DNA record, to be processed to the EHR system. For clarification, DNA is a source of patient information and nucleotides consisting of five-sided sugar, a phosphate group, and a base. There are four different types of nucleotides, each defined by a specific base: A (Adenine), C (Cytosine), G (Guanine) and T (Thymine) [2]. The nucleotides depend on the DNA sequencing order, which indicates how important the way of processing the critical data among the entities is. This paper focuses on how the DNA record can be transferred reliably to the final location; thus, we will skip further discussion for the DNA sequencing concept.

Coding schemes are popular methods in todays' networks for sending information successfully to the end destination. There are various methods invented until now, but the general idea behind all diverse schemes is adding some predefined redundancy to the useful part of information in order to prevent the data from dealing with some errors and modifications that can appear during the transmission process. In our paper, we focus on two different coding methods for processing the data, namely a Hamming code and the Reed-Solomon code [3]. Both schemes, through examples, are applied to the same piece of DNA record and

accordingly, the number of error detection and corrections are calculated and compared. The operation mentioned previously shows which code scheme performs better for DNA record processing reliably and securely to the EHRs.

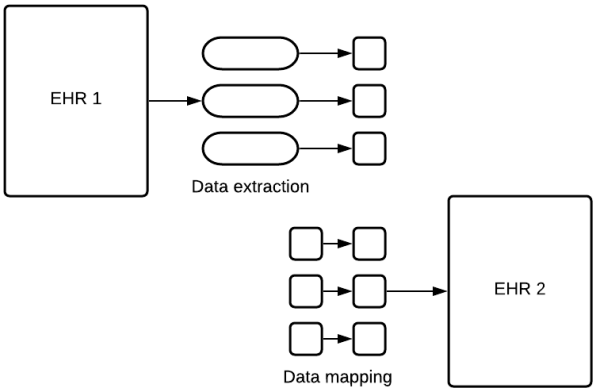

Fig. 2 EHR data processing

Nevertheless, this paper is organized as follows: Section II surveys the concepts related to EHR systems and explains different techniques for patient data processing without significant modifications. Section III and IV, respectively, explain how encoding and decoding work with Hamming and Reed-Solomon code for patient data transmission. Section V summarizes and compares the results from the previous sections, and section VI concludes the paper.

II. Related Concepts

Reliability and security are fundamental concerns in any healthcare system. Different researches have proposed many security reference architectures. One of them is given in [4] by proposing this kind of architecture that can be seen as a base point to study security threats and their characteristics. Paper [5] elaborates on specific reliable architecture for patient data and healthcare services management. Consequently, the benefits of existing EHR systems became better understood, and the performance gains associated with EHR adoption were clarified. [5]

Another way of looking at security in EHR systems is the attempt to protect physician's services and patient data from various attacks done by third parties. Paper [6] defines different security aspects related to authorization, authentication, encryption and access control for EHR systems. Issues around data security, trustworthiness and privacy today are under greater focus than ever before. As a result, many techniques for data protection have been developed over the past 20 years [6]. Reference [7] provides a broad perspective about the variety of research that can contribute to developing effective and efficient data protection technologies.

Other aims for the creation of the EHR are transparency, openness, reliability, performance and scalability. Implementing such systems with the objectives mentioned above is elaborated in [8]. The first EHR systems were implemented in 2001 using the concept of paper-based records. Today EHR systems are quicker, more secure and more accurate than the traditional paper-based records because they consider the difference in age, gender, job title, previous computer experience and education levels [9].

The increased rate of adoption of EHR systems at hospitals rather than paper-based records demonstrates the efficiency of how the patients are treated. The advantages are enormous because hospitals want to deliver quality healthcare for their patients without severe cost overruns [10]. The usage of the EHR systems greatly increases the precision and comprehensiveness of medical data, which will enhance standards and disease prevention capabilities. Databases consisting of medical records make data more easily shareable between providers and organizations [11].

Many systems designs, including EHR systems, have been proposed to address information availability challenges. Considerations for security in protecting data are mostly ad hoc and patch efforts which may not be well thought out as part of an overall security architecture. Researchers in [12] show that attribute-based authorization can be a critical architectural component for protecting healthcare systems and their users from insider attacks. Smart healthcare services are a great boon and are dominantly used by patients, doctors and other healthcare providers. Since most data is stored in cloud servers, there is an imminent need to safeguard them from unauthorized access. Existing smart health solutions, i.e. e-health cloud preserving cryptographic and non-cryptography mechanisms, provide a privacy aspect in the cloud. The evolution of such security mechanism can make health care data more secure and sustainable [13]. The intent of chapter [14] has been to outline how EHR systems work and how different mechanisms support such systems' operations to avoid security issues. Managing and storing the Big Data in EHR systems is a big challenge. Therefore, the paper [15] provides an overview of all methods used in order to achieve data security in different systems. Different coding techniques, encryption algorithms and classifications were done to determine which security method is adequate to deal with what kind of attack. A well-known group of popular error-correcting codes is also considered for DNA record protection in EHRs. Some researches can be found in references [18-20].

The inventions of such systems improve the worth and effectiveness of healthcare. The high satisfaction of medical data collected in such systems results in the functionalities available for prescribing drugs [16]. In [17], a novel method was proposed, which was used to construct and securely store shadows of medical images. The experimental results demonstrate that using (7, 4) Hamming code gives a more desirable blurring effect than using (15, 17) Hamming, because the scheme that was proposed by the authors runs much faster at low computational costs which is suitable for mobile devices or small size hospitals or clinics. All of the concepts mentioned above explain different ways for patient data security. But, through our investigation, we gain knowledge that we need to compare two coding techniques

with different performances, as a novel method, to give a better solution for patients' data security in EHR systems. This is why we implemented the Hamming code and Reed-Solomon code for DNA data transmission as critical patient records that should be processed and stored in the EHR without any single modification. The constructions of the two codes are elaborated in [3], [18-20].

III. HAMMING CODE

This section uses a concrete example to explain how the Hamming code encodes and decodes DNA records. Then, it calculates the number of errors detected and corrected during the data transfer process to other EHR systems.

A. Hamming Code applied to DNA record

We considered the Hamming (31, 26) code to encode the data consisted of the strings **s**=*hello*. This string is taken for simplicity to represent the example, but in reality, it should be seen as a sensitive DNA record. For the encoding process of this code, we need to construct a particular generator matrix. For this purpose, we use the matrix *A* with dimension 5x26 given in equation (1) and an identity matrix with dimension 26x26. Thus the *generator matrix G* with dimension 26x31 is obtained by taking $G = [\, I_{26} \; -A \,]$. Additionally, we construct the *parity-check* matrix $\boldsymbol{H}$ with dimension 31x5 by taking $H = \begin{bmatrix} A \\ I_5 \end{bmatrix}$, where *A* is the matrix from (1) and I_5 identity matrix with dimension 5x5.

In the supplementary information of [3], the Python code used for encoding and decoding DNA data storage was given. To understand these two procedures, we will analyze and discuss them more thoroughly in this paper.

B. Encoding data string to DNA record using Hamming (31, 26) code

This section demonstrates all steps needed for data encoding using the Hamming (31, 26) code to save the DNA record and transmit it to the EHR system safely to the final destination.

Step 1. Firstly, the string **s** = *hello* is converted to numerical string. The conversion procedure is following: the *UTF-8* encoding is used in order to convert all of the letters from the string **s** to *ASCII* symbols. Those numerical symbols are then converted to *base 4* numbers and they are concatenated. The codes in this paper are applied to quaternary digits {0, 1, 2, 3}, known as *quads*. So, the resulting message of 20 quads is denoted as

$$\boldsymbol{m} = 12201211123012301233.$$

The process of string-number conversion in details can be seen in Table 1.

Step 2. In order to count all unique symbols in one string we need to add a *cyclic redundancy check* (CRC) that contains the Secure Hash Algorithm known as SHA-256. This is put into *base 4* form and the 6 right-most quads are taken. The result of this step is denoted by

$$\boldsymbol{h} = 110213.$$

After that the outputs $\boldsymbol{m}$ to $\boldsymbol{h}$ are concatenated obtaining message with 26 quads

$$\boldsymbol{a} = 12201211123012301233110213.$$

letter	***ASCII***	***base 4***
h	*104*	*1220*
e	*101*	*1211*
l	*108*	*1230*
l	*108*	*1230*
o	*111*	*1233*

Table 1*: Step 1 –Encoding data to DNA using Ham (31, 26) code*

Step 3. The next step is when the generator matrix $\boldsymbol{G}$ comes into play which is used in order to encode the message $\boldsymbol{a}$**.** Hence, by multiplying $\boldsymbol{a}$ and $\boldsymbol{G}$ we get the following result with 31 quads in total

$$\boldsymbol{aG} = \boldsymbol{b} = 122012111230123012331102132113 1.$$

Step 4. To make sure that errors can be detected and corrected we need to know that not all words are codewords. Hence, we should add a parity check quad $\boldsymbol{p}$ which is 3 in our case (by performing on $\boldsymbol{b}$ modulo operation 4), resulting with the final codeword with 32 quads presented as

$$\boldsymbol{c} = 3122012111230123012331102132113 1.$$

Step 5. The last step is when we want to store the string as autonomous DNA record in the EHR. In order to convert $\boldsymbol{c}$ to DNA we map each number {0, 1, 2, 3} to the appropriate letter {A, C, G, T}. As a result we get the sequence

$$\boldsymbol{d} = T\ CGGACGCCCGT\ ACGT\ ACGT\ T\ CCAGCT\ GCCT\ C.$$

The process of encoding data to DNA using Hamming (31, 26) code is finished when all of the above steps are completed.

C. Decoding DNA record to data string using Hamming (31, 26) code

This section will demonstrate all of the steps required for DNA record decoding using the *Hamming (31, 26)* code in order to transmit the DNA record to other EHR systems and successful use it in a secure manner at the final destination.

Step 1. Suppose a DNA strand $\tilde{\boldsymbol{d}}$ is retrieved after sequencing and that error might have occurred. Therefore, we need to convert $\tilde{\boldsymbol{d}}$ back to *quads*.

Step 2. Secondly, the *parity-check* matrix $\boldsymbol{H}$ is used in order to calculate an error vector $\boldsymbol{e} = \tilde{\boldsymbol{b}}\boldsymbol{H}$ when $\tilde{\boldsymbol{c}}$ is converted into $\tilde{\boldsymbol{b}}$ and the *parity quad* $\tilde{\boldsymbol{p}}$ and $\tilde{\boldsymbol{b}}$ are decoded. In this way it is possible to find out the error position and error value.

Step 3. The next step is to fix and decode the data into $\tilde{\boldsymbol{b}}_{dec}$ which is done by subtracting (*modulo 4*) the error value from the *quad* in order to obtain the original *quad*.

Step 4. The fixed data $\tilde{\boldsymbol{b}}_{dec}$ will help us to check for *parity quad* $\tilde{\boldsymbol{p}}$ and based on the previous data the type of the error is determined and returned.

Step 5. By implementing *CRC* we can see if there are any errors left in $\tilde{\boldsymbol{a}}$. In order to provide this step, $\tilde{\boldsymbol{a}}$ is split into the first 20 *quads*, denoted by $\tilde{\boldsymbol{m}}$, and the last 6 *quads*, denoted by $\tilde{\boldsymbol{h}}$, where *CRC* for $\tilde{\boldsymbol{m}}$ is computed and compared to $\tilde{\boldsymbol{h}}$. This check will return *True* or *False*.

$$A=\begin{bmatrix} 1&1&0&1&1&0&1&0&1&0&1&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \\ 1&0&0&1&0&1&1&0&0&1&1&0&1&0&0&1&1&1&0&0&1&1&0&0&1&1 \\ 0&1&1&1&0&0&0&1&1&1&1&0&0&1&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&0&1&0&1&1&1&1&1&1&1&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \end{bmatrix} \quad (1)$$

Step 6. The last step is to convert $\widetilde{\boldsymbol{m}}$ to $\tilde{\boldsymbol{s}}$ in reverse order of *Stage 1* of encoding $\tilde{\boldsymbol{s}}$ until there are no more *quads* to convert. The final string is stored in $\tilde{\boldsymbol{s}}$ and is returned with the result of the *CRC* check.

The process of decoding DNA record using Hamming (31, 26) code is finished when all of the above steps are completed.

D. Example of error

This section demonstrates how the appearance of one error: non-parity base during the process of transmission to the final destination is handled by the Hamming (31, 26) code. Note that the type of the error in our case is correctable error which is denoted by 2.

$\tilde{\boldsymbol{d}}$ = T AGGACGCCCGT ACGT ACGT T CCAGCT GCCT C

$\tilde{\boldsymbol{c}}$ = 3 0220 1211 1230 1230 1233 110213 21131

$\tilde{\boldsymbol{b}}$ = 0220 1211 1230 1230 1233 110213 21131

err_type = 2

e = [33000]

(*err_pos, err_val*) = (0, 3)

$\tilde{\boldsymbol{a}}$ = 1220 1211 1230 1230 1233 110213

$\widetilde{\boldsymbol{m}}$ = 1220 1211 1230 1230 1233

CRC pass = *True*

$\tilde{\boldsymbol{s}}$ = h e l l o

E. Analysis of the encoding and decoding process with Hamming (31, 26) code

The encoding and decoding process of using the *Hamming (31, 26) code* has three ways of securing the data: *Parity check* matrix $\boldsymbol{H}$, *parity quad* that was added and *CRC* pass. Hence, suppose one error occurred during sequencing and $\tilde{\boldsymbol{d}}$ is retrieved. Using the *parity-check* matrix $\boldsymbol{H}$ it will find and correct that error. However, if the error is detected in *parity quad* $\tilde{\boldsymbol{p}}$ it will not affect the decoding process and $\boldsymbol{s}$ can still be retrieved.

The second scenario is that two errors occurred in $\tilde{\boldsymbol{d}}$ and both are not in $\tilde{\boldsymbol{p}}$. In this case $\boldsymbol{H}$ will detect that there is an error, but if $\boldsymbol{e}$ contains different non-zero values, then multiple errors have occurred, but the code is not able to correct more than one error. Hence, $\boldsymbol{H}$ can only detect and correct one error, so it will incorrectly decode $\tilde{\boldsymbol{d}}$**.** Now, the parity quad $\tilde{\boldsymbol{p}}$ comes into play to check whether the received $\tilde{\boldsymbol{d}}$ matches with the parity. All calculations are done base on the incorrectly decoded sequence $\tilde{\boldsymbol{d}}$. If multiple errors occur, that match cannot be not performed, but nevertheless, the CRC usually still detects those errors.

IV. Reed-Solomon

This section uses a concrete example to explain how the Reed-Solomon code encodes and decodes DNA records. Then, it calculates the number of errors detected and corrected during the data transfer process to other EHR systems.

A. Reed-Solomon applied to DNA record

The *Reed-Solomon* codes are used in order to encode the data and the main goal of this technique is to provide correction of multiple errors. In order to apply the *Reed-Solomon* to DNA records, the field *F (256)* is used which requires to choose *n* and *k* such that $\frac{n-k}{2}=2$. In our case it is logical to choose *n* = 255 and *k* = 251, but the original string $\boldsymbol{s}$ is consisted of 5 symbols which means that it is more convenient to choose *k* = 5 [21]. This is the main reason why a *shortened Reed-Solomon code* is used.

Shortening a *RS (n, k)* code with minimum distance d by a symbols will yield a *RS(n−a, k−a)* code with minimum distance *d*, where *a* is a primitive element. Therefore, the *RS (255,251)* code is shortened into a *RS (9,5)* code. Because the encoding and decoding schemes of the *Reed-Solomon* code are fairly complicated we decided to implement the unireedsolomon 1.0 package available on *PyPI* under an *MIT* license that can encode and decode a possible shortened Reed-Solomon code over *F (256)* for a given *n* and *k*.

B. Encoding data string to DNA record using RS (9, 5) code

This section demonstrates all steps required for data string encoding using the *RS (9, 5)* code to save the DNA record and transmit it to the EHR system safely to the final destination.

Step 1. Firstly, the string **s** = *hello* is converted to *ASCII* symbols, and then, using the field *F (256)* the symbols are converted to values between 0 and 255. So, the resulting message is denoted by

$$\boldsymbol{m} = 104\ 101\ 108\ 108\ 111.$$

Note that the length of $\boldsymbol{m}$ is five in this case, the symbols consist of 3 digits.

Step 2. Secondly, the message $\boldsymbol{m}$ is encoded with *RS(9,5)* code with the previously mentioned package using a generator polynomial *q* which as a result will return a string with 9 symbols given as

$$\boldsymbol{b} = 104\ 101\ 108\ 108\ 111\ 127\ 24\ 174\ 193.$$

Step 3. In this step all of the *ASCII* symbols are converted to *base 4* numbers and they are concatenated and the following sequence is obtained

$$\boldsymbol{c} = 122012111230123012331333012022323001.$$

If we compare the result what we have obtained in *Section III.B* we can conclude that the value of $\boldsymbol{s}$ is changed from 32 to 36 *quads*.

Step 4. The last step is to convert $\boldsymbol{c}$ to autonomous DNA record ready for storing or transferring to other EHRs. The conversion is done by mapping the numbers {0,1,2,3} into appropriate letters $\{A, C, G, T\}$, respectively. As a result we get

$\boldsymbol{d}$ = CGGACGCCCGT ACGT ACGT T CT T T ACGAGGT GT AAC.

The process of encoding data string to DNA record using *RS (9, 25)* code is finished when all of the above steps are completed.

C. Decoding DNA record to data string using RS (9, 5) code

This section will demonstrate all of the steps needed for DNA record decoding using the same *RS (9, 5)* code in order to transmit the DNA record to other EHR systems and successfully use it in a secure manner at the final destination.

Step 1. Suppose a DNA strand $\tilde{\boldsymbol{d}}$ is retrieved after sequencing and that error might have occurred. Therefore, we need to convert $\tilde{\boldsymbol{d}}$ back to *quads* to gain $\tilde{\boldsymbol{c}}$.

Step 2. Secondly, $\tilde{\boldsymbol{c}}$ is divided into parts of 4 *quads* and each of them is read as a *base 4* number and converted to *ASCII* symbol, and after that it is converted to element sequence returned from the field *F (256).* When we put both together we get that $\tilde{\boldsymbol{b}}$ has length 9.

Step 3. The next step is to fix and decode the data into $\tilde{\boldsymbol{b}}$ which will give us the value of $\tilde{\boldsymbol{b}}_{dec}$. This process is done via the *Reed-Solomon* decoding function from the package mentioned above.

In order to check that $\tilde{\boldsymbol{b}}_{dec}$ is a valid code, or is decoded without any errors, the *RS chec*k is introduced. All codewords are multiples of the generator polynomial *g*, so $\tilde{\boldsymbol{b}}_{dec}$ is a codeword if *g* divides $\tilde{\boldsymbol{b}}_{dec}$. This check will return *True* or *False*.

Step 4. The last step is to translate the ASCII symbols back to characters to form string $\tilde{\boldsymbol{s}}$.

The process of decoding data to DNA using *RS (9, 25)* code is finished when all of the above steps are completed.

D. Example of error

This section demonstrates how the appearance of *two errors in different parts* is handled by the *RS (9, 5)* code.

$\tilde{\boldsymbol{d}}$ = AGGAAGCCCGT ACGT ACGT T CT T T ACGAGGT GT AAC

$\tilde{\boldsymbol{c}}$ = 0220 0211 1230 1230 1233 1333 0120 2232 3001

$\tilde{\boldsymbol{b}}$ = 40 37 108 108 111 127 24 174 193

$\tilde{\boldsymbol{b}}_{dec}$ = 104 101 108 108 111 127 24 174 193

RS check = True

$\tilde{\boldsymbol{m}}$ = 104 101 108 108 111

$\tilde{\boldsymbol{s}}$ = h e l l o

E. Analysis of the encoding and decoding process with Reed-Solomon (9, 5)

The encoding and decoding process of using the *Reed-Solomon (9,5)* and choosing the parameters *n* and *k* specifically can determine how many errors the code can correct in the field which is applied. However, in our case we need to correct 2 base errors. By applying the scheme to the DNA records, it can correct up to 8 base errors because the Reed-Solomon code works in field *F(256)* which can correct 3 errors in the ASCII symbols. Note that the main goal to implement this type of code is the ability to correct multiple errors if they occur into the data during the transmission process.

V. Comparison

In this section, the results from the previous sections are summarized and compared. When analyzing the error detection and correction, the *Reed-Solomon* code clearly outperforms the *Hamming code* since it can correct 2 errors instead of 1. Therefore, as explained in the previous section, the Reed-Solomon code in many cases can correct even more than 2 errors when they occur in the same DNA records that correspond to one symbol of *F(256).*

The main difference between the encoding schemes of the *Hamming* and *Reed-Solomon codes* is the order in which the data is encoded and is converted to *quads*. For the *Hamming code*, the string **s** was first converted to *quads* before the *CRC*, and the matrix G was used to encode the message. On the other side, for the *Reed-Solomon code*, the string was firstly encoded and converted to *quads* afterwards, which also changed the order of the decoding steps. Table 2 gives the differences and similarities between both coding schemes used in EHR systems.

Hamming Code	***Reed-Solomon Code***
Defined in the binary field	Defined in the non-binary field
Correct one dedicated error	Correct multiple dedicated errors
Unique steps for Encoding/Decoding process (see Section III)	Unique steps for Encoding/Decoding process (see Section IV)
Poor Performances and process small data	Better Performances and process bigger data

Table 2*: Hamming Code vs. Reed Solomon applied in EHR systems*

VI. Conclusion

DNA record is very sensitive patient information. Keeping this data in its original format in the EHR systems and transfer it to other medical centers unchanged for preparing health treatment is an important issue which needs to be addressed. Introducing coding schemes for storing and processing data can guarantee the reliability and security of those systems. Therefore, in this paper, we examine and demonstrate the usefulness of two different code schemes, the Hamming and Reed-Solomon. The methods used in this paper were based on a *Ham (31, 26) code* and a *RS (9, 5) code*. Both schemes were introduced with descriptions for the encoding and decoding steps. Through examples this paper investigated to see how they responded to data errors.

The conclusion is that the *Reed-Solomon* outperform the *Hamming code. The RS code* excels in other important qualities like error correction, and its implementation is not as simple as the implementation of the *Hamming code*. On

the other side, the *Reed-Solomon code* has more potential to work properly on more enormous data sets where the number of errors that the code is able to correct can increase. Counting up all these arguments, it is fair to conclude that the *Reed-Solomon code* is more suitable for transmitting the DNA record to the EHR system than the *Hamming code*.

REFERENCES

[1] Mitreska I., Marina N., Capeska Bogatinoska D. (2021) Electronic Health Records System for Efficient Healthcare Services. In: Badnjevic A., Gurbeta Pokvić L. (eds) CMBEBIH 2021. CMBEBIH 2021. IFMBE Proceedings, vol 84. Springer, Cham. https://doi.org/10.1007/978-3-030-73909-6_

[2] A. Blanco and G. Blanco, "Nitrogenous Base", Science Direct, 2017

[3] C. N. Takahashi, B. H. Nguyen, K. Strauss, and L. Ceze, "Demonstration of End-to-End Automation of DNA Data Storage," Scientific Reports, vol. 9, pp. 4998, 2019

[4] S. Mahmood, M. J. Khan and S. Anwer, "Applications of Security Reference Architectures in Distributed Systems: Initial Findings of Systematic Mapping Study", Tenth International Conference on Software Engineering Advances, 2015

[5] J. A. Milstein, J. Everson, S. D. Lee, "EHR Adoption and Hospital Performance: Time-Related Effects", Health Research and Educational Trust, vol. 50, pp. 1751-1771, 2015

[6] I. Shadmanov and K. Shadmanova, "Summarization of Various Security Aspects and Attacks in Distributed Systems: A Review", Advances in Computer Science: an International Journal, vol. 5, no. 19, January, 2016

[7] E. Bertino, "Introduction to Data Security and Privacy", Springer, pp. 125-126, September, 2016

[8] G. F. Elkabbany and M. Rasslan, "Security Issues in Distributed Computing System Models", IGI Global, 2017

[9] K. E. M. Msiska, A. Kumitawa and B. Kumwenda, "Factors affecting the utilization of electronic medical records system in Malawian central hospitals", M. M. Journal, pp. 247-253, September, 2017

[10] D. Wani and M. Malhota, "Does the meaningful use of electronic health records improve patient outcomes?", Journal of Operations Management, vol. 60, pp. 1-18, June, 2018

[11] C. S. Kruse, A. Stein, H. Thomas and H. Kaur, "The use of Electronic Health Records to Support Population Health: A Systematic Review of the Literature", M. M. Journal, September, 2018

[12] V. C. Hu, D. R. Kuhn and D. F. Ferraiolo, "Access Control for Emerging Distributed Systems", National Institute of Standards and Technology, 2018

[13] S. Chenthara, K. Ahmed, H. Wang and F. Whittaker, "Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing", IEEE Access – Multidisciplinary open access journal, May 2019

[14] E. Lupu, "Distributed Systems Security", The National Cyber Security Centre, October, 2019

[15] N. Paunkoska and A. Risteski, "Security in distributed storage systems – Encryption algorithm vs. Coding schemes", Journal of Electrical Engineering and Information Technologies, November, 2019

[16] T. R. Schopf, B. Nedrebq, K. O. Hufthammer, I. K. Daphu and H. Laerum, "How well is the electronic health record supporting the clinical tasks of hospital physicians? A survey of physicians at three Norwegian hospitals", BMC Health Services Research, December, 2019

[17] L. Li, C. Chang, J. Bai, H. Le, C. Chen and T. Meen, "Hamming Code Strategy for Medical Image Sharing", Applied System Innovation – An Open Access Journal from MDPI, January 2020

[18] M. Blawat, K. Gaedke, I. H¨utter, X.-M. Chen, B. Turczyk, S. Inverso, B. W. Pruitt, and G. M. Church, "Forward Error Correction for DNA Data Storage," Procedia Computer Science, vol. 80, pp. 1011–1022, 2016

[19] R. N. Grass, R. Heckel, M. Puddu, D. Paunescu, and W. J. Stark, "Robust chemical preservation of digital information on DNA in silica with error-correcting codes," Angewandte Chemie - International Edition, vol. 54, pp. 2552–2555, 2 2015

[20] L. Organick, S. D. Ang, Y.-J. Chen, R. Lopez, S. Yekhanin, K. Makarychev, M. Z. Racz, G. Kamath, P. Gopalan, B. Nguyen, C. N. Takahashi, S. Newman, H.-Y. Parker, C. Rashtchian, K. Stewart, G. Gupta, R. Carlson, J. Mulligan, D. Carmean, G. Seelig, L. Ceze, and K. Strauss, "Random access in large-scale DNA data storage," Nature Biotechnology, vol. 36, pp. 242–248, 2 2018

[21] E. Slingerland, "DNA Data Storage Hamming and Reed-Solomon Codes", Delft, Nederlands, June 2019

Journal of Emerging Computer Technologies
Research Article
Received: *2021-11-20* | ***Reviewing:*** *2021-11-20* & *2021-12-20*| ***Accepted:*** *2021-12-21* | ***Online:*** *2021-12-21* | ***Issue Date:*** *2021-12-31*

Automatic Movie Rating by Using Twitter Sentiment Analysis and Monitoring Tool

Feriştah Dalkılıç
Department of Computer Engineering
Dokuz Eylül University
İzmir, Turkey
feristah@cs.deu.edu.tr
0000-0001-7528-5109

Ayşe Çam
Department of Computer Engineering
Dokuz Eylül University
İzmir, Turkey
ayse.cam@ceng.deu.edu.tr
0000-0002-7714-2117

***Abstract*— Today, due to the intense use of social media platforms such as Twitter by all segments of today's technology, people have begun to share their views, ideas, and feelings through these media. It is possible to discover mighty valuable knowledge from this enormous resource. This study has emerged to assist users in making choices by evaluating emotions about TV series and movies that have recently appeared on social platforms, using ideas and feelings. The textual tweet data was preprocessed and cleaned of noise by using natural language processing techniques. Tweets were tagged using the Bert-based model according to the content of the Turkish TV series and movie comments, and their polarities were calculated. Machine learning models including Naïve Bayes (NB), Support Vector Machines (SVM), Random Forest (RF); Bagging and Voting, which are among the general ensemble algorithms, were trained for sentiment analysis by taking the obtained polarity values. The voting algorithm gives the best accuracy at 87%, while the Support Vector Machines give the best area under the receiver operating characteristics curve (AUC) of 0.96. A web application was developed by using Flask to monitor sentiment scores via hashtags (#).**

Keywords—sentiment analysis, machine learning, natural language processing, social data science

I. INTRODUCTION

Today, due to the increasing internet use, users communicate through social networks. Social networks have become the easiest way people can express themselves and spread their ideas. People update their status in every activity they do, share their photos, and instantly share their thoughts about the TV series, movies and TV shows they watch. For this reason, issues such as the processing of data received from social networks gain importance day by day. Most of the evaluations in this study are on Twitter, new TV series and movies are on Netflix, AmazonPrime, BlueTV etc. published on platforms.

Several studies have been conducted to extract sentiment from social media data, especially from Twitter data in the last decades. But very few of these studies are in Turkish [1]. In this study, the tweets in Turkish that have hashtags (#) with movie titles were evaluated, classified, and rated as positive, negative, or neutral. Along with these, the total number of people who tweeted, the first user to use the hashtag showed how it affects women and men. Twitter API was used to access and collect Twitter data. The tweets were stored in MongoDb with NoSQL infrastructure. The following stages were applied to tweets pulled according to hashtags, respectively: Words were normalized and converted to lowercase. String tokenization was applied to texts, stop words were removed. Since the tweets were found without tags, they were tagged with certain models. A rating system was proposed to show the likes and dislikes rates over many different tweets and comments for new movies and series, such as IMDB ratings, on a single site.

II. RELATED WORKS

In recent years, sentiment analysis and opinion mining studies have become a popular subject in the field of natural language processing (NLP). Social media reviews, forums, microblogs, and product reviews have been used in many of the studies carried out in this field. Twitter data has been analyzed to understand social media users' opinions on various issues in daily life. Zimbra et al. gave a detailed survey of Twitter sentiment analysis applications [2]. Wang et al. used Twitter data about the 2012 US presidential election to develop a system for real-time sentiment analysis [3]. Abalı et al. detected the problems of citizens and extracted the locations of complaints from Turkish tweets collected from the Aegean Region of Turkey [4]. Chakraborty et al. handled COVID-19 related tweets during two distinct pandemic times to analyze the sentiment tendency of tweets [5]. Pant et al. performed the prediction of Bitcoin's volatile price by analyzing sentiment on Twitter [6]. A sentiment analyses of the automotive industry tweets was presented by Shukri et al. to extract the polarity and emotions classification towards the automotive classes [7].

Several different techniques have been used in sentiment analysis and opinion mining studies hitherto. Some studies were conducted on lexicon-based methods while others were conducted on machine learning-based methods. These techniques have been combined in some recent studies.

Lexicon-based methods use a sentiment dictionary to detect the sentiment tendency of text. Quan and Ren conducted a feature-based sentiment analysis study on product reviews [8]. For feature extraction, they first determined all names in the interpretation as candidate traits, then they used Term Frequency-Inverse Document Frequency and Pointwise Mutual Information (PMI) methods together to determine the level of relationship of these candidate features with the product. After determining the product features, they used a commitment parser to detect emotion expressions and emotion polarities. They tested their proposed method on their comments on digital cameras, cell phones, mp3 players, and routers. In these tests, they achieved success rates between 61% and 89% in feature extraction and between 66% and 77% in emotion classification. In their study, Atan and Çınar used news texts published in different news sources in 2014 regarding BIST30 companies traded on Borsa Istanbul as a data set [9] and converted the expressions in the news content into numerical values with the help of a sentiment dictionary translated into Turkish. Then, the relationships between these

Cite (APA): Dalkilic, F., Cam, A. (2021). Automatic Movie Rating by Using Twitter Sentiment Analysis and Monitoring Tool. *Journal of Emerging Computer Technologies*, 1(2), 55-60.
Volume:1, **No:**2, **Year:** 2021, **Pages:**55-60, December 2021, Journal of Emerging Computer Technologies

numerical scores and the company values formed in the market in the same period were analyzed. The main result that emerges is that there are significant relationships between the news published in financial markets and their emotional tone and financial values. Karagöz and Gürsoy used the tweets written about the programs broadcast on a TV channel in an eight-month period as a data set [10]. Sentiment analysis revealed that the messages about the channel and the program included in this data set contained emotions classified as positive, negative, or neutral. With this information, channel managers were able to make predictions for program managers and it was stated that they could develop relevant strategies in this direction.

In some of the recent studies, machine learning methods are used to identify the sentiment polarity in texts [11]. Both unsupervised learning-based clustering techniques and supervised learning-based classification techniques of machine-learning have been employed for sentiment analysis. Li et al. tried to determine the locations of incidents such as murder, accident, and disease by predicting the time and place using tweets. While ranking similar tweets, they used clustering methods. Finally, they used a Linear Regression (LR) model to score the importance of tweets [12]. Tuzcu used a data set containing reader comments taken from an online book sales site to make emotion classifications with classification algorithms [1]. An emotion classification was performed with Multi-Layer Perceptron (MLP), NB, SVM, and LR algorithms. Although all algorithms have done well, MLP was the algorithm that performs the best. Basiri et al. proposed a method based on a fusion of four deep learning and one traditional supervised machine learning model on coronavirus-related tweets for sentiment analysis [13]. They stated that their model is better than four individual deep models and the DistilBERT model.

Hybrid methods merge machine learning and lexicon-based methods to recognize text emotion. Torres developed a sentiment analysis service on student-generated comments in Spanish. The original system performs the natural language processing task to determine the sentiment associated with a text. SVM, Naïve Bayes, logistic regression, and decision tree machine learning models have been used for sentiment classification. The results showed that machine learning-based methods outperformed the original system [14]. Kaynar et al. used Naïve Bayes, Central Based Classifier, Multi-Layer Perception (MLP), and SVM for sentiment analysis of movie reviews in IMDB [15]. According to experiments, it is seen that MLP and SVM outperform both training and test sets. In the training dataset, MLP performed better with an 89.73% correct classification rate while both classifiers showed almost the same performance with a correct classification rate of around 75% for the test data set. Patel and Passi used the tweets about the 2014 World Cup soccer tournament held in Brazil to analyze the emotion of people all over the world by combining lexicon-based and machine learning methods [16]. They obtained the best accuracy of 88.17% by the Naïve Bayes classifier, and the best AUC of 0.97 by the random forest classifier.

III. METHOD

In this study, we performed natural language processing techniques including word tokenization, stop word elimination, word stemming, and lemmatization. Along with these, spell checkers have been applied to correct spelling mistakes. While tagging tweets, the Bert model was activated with the support of Google Colab's GPU augmentation, and a training dataset of 3 sentiment moods was prepared. TF-IDF vectorizer was used to create the polarities of the words separated into their stems, and these digitized values were made ready for use in machine learning algorithms. The general flow of the proposed method is given in Fig. 1.

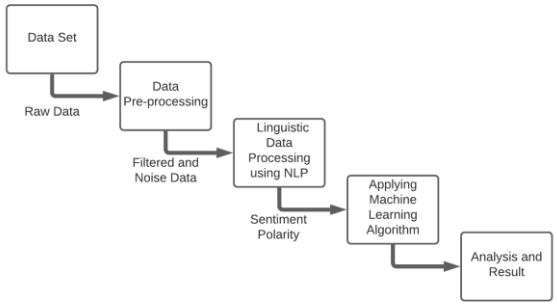

Fig. 1. Flowchart of the proposed method.

A. Dataset

In the scope of this study, a dynamic data set consisting of tweets with hashtags related to movies and TV series that have been published recently was collected. Tweets were pulled according to keywords by accessing the Twitter API and using the Tweepy library. Datetime and base64 libraries were used to access instant tweets. MongoDB, a NoSQL database, was preferred to store large amounts of data and perform fast searches [17]. MongoDB keeps adding, updating, deleting, and searching non-relational data on the file system in Json format. Sentiment analysis studies were conducted with a total of 19,398 tweets.

B. Preprocessing Tasks

The real meaning and sentiment of the text data can only be derived correctly if the data are cleaned from noise or irregular patterns. To perform analytical operations in tweets, words must be digitized and measurable. For this purpose, it is important to make the words as simple as possible to measure the frequency of the words.

TABLE I. ALGORITHM FOR THE PREPROCESSING OF TWITTER COMMENTS

STEP	OPERATION
1	By using regular expression techniques, all URLs are replaced with the 'URL' keyword
2	All '@username' terms are replaced with the 'AT_USER' keyword
3	All #Hashtags and RT are eliminated from the text
4	Capitalization conversion to lowercase
5	Double spaces and double characters are corrected
6	Turkish characters [^A-Za-zığüşöç] are allowed
7	Predefined special characters (: n | [ ] ; : {} – + ( ) < > ? ! @ # % *,) are eliminated
8	Comment texts are tokenized
9	Stop words are eliminated

The crawled tweets contain URLs, hashtags \#", annotation \@" and retweets \RT" in addition to text data. Before applying machine learning techniques to the text data, text input must be tokenized. Preprocessing was performed by passing the data through the steps of capitalization conversion, elimination of punctuation marks, and elimination of stop words. The Turkish corpus of the NLTK library was used in the filtering of the stop words. The Word Punct Tokenizer module from the NLTK package was used to split the text into tokens and delete punctuation. Preprocessing steps applied to tweets are given in Table 1.

There are many natural language processing libraries developed for Turkish, the Zemberek project was preferred for its features and ease of use. After cleaning the data by using several well-known techniques (outlier detection, …), the data got ready to be labeled. There may be some spelling mistakes or different spelling in raw words due to the Twitter environment. Using SpellChecker from the Zemberek library, it was checked whether the words were spelled correctly. If a spelling mistake was detected, the first suggestion was used to correct it. It was also added to the temporary empty list.

The initial unconjugated form of words is called lemma. So, each word has to be transformed its lemma form before labelling. This is the essential aim of lemmatization that parses the lemma form of the word by finding out the suffixes and/or prefixes added or prepended to the word, and in our study Zemberek library was our valuable assistant.

C. Data Labeling

After the data was pre-processed; 19,398 tweets were tagged as positive, negative, and neutral in order to train the model. At this stage, the BERT model developed by Google was used [18]. First, a small model was created using the BERT algorithm, and this model was run on 19,398 tweets. In contrast to the superficial language processing that goes from right to left and left to right, the BERT algorithm found the relationship of each word with the other word, resulting in complex but more accurate hashtag tweets.

After tagging the tweets, Fig. 2 is prepared by using the ratio of positive, negative and neutral results. Tweets that are only in the Turkish language were analyzed and the tweets in other languages were ignored. The reason why there are so many negative tweets is due to users' reactions to events in the scenes. Some sample pre-processed and tagged tweets can be seen in Fig. 3.

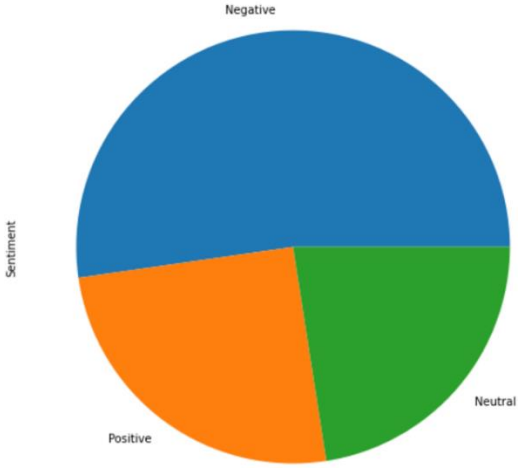

Fig. 2. Sentiment distribution of tweets.

Tweet	Sentiment	Analysis
yalan söyleyeyim üzgünüm yanım kopmuş kanamış ...	-1	Negative
ilker boşandıktan gerçekten zafer işareti yapt...	-1	Negative
hande saf kötüsün [redacted] kızı saçını başını yolas...	-1	Negative
şte budur adaletsiz guen osmanbey çocuklarakıy...	1	Positive
[redacted] kuzen işi var elanın odasında masumiyet ...	-1	Negative
...	...	...
beynim yandı sizce suçlu masumiyet	-1	Negative
kisinide izlemiyorum	0	Neutral
linç kültürünü iyi anlatan dizi bence kız kend...	-1	Negative
masumiyet hülya avşar filtreli görünce kime be...	0	Neutral
kadının büyük düşmanı yine kadın masumiyet	-1	Negative

Fig. 3. Sample pre-processed and tagged tweets

D. TF-IDF Model

Before moving on to classification modeling with machine learning, data should be represented numerically. In this part of the study, we digitized the data using the term frequency-reverse document density (TF-IDF) model. The more the term is repeated in the document, the higher the TF-IDF value. In the coding part, TfidfVectorizer class was used to convert TF-IDF feature matrix. Bigrams and unigrams were included using ngram_range in TfidfVectorizer.

Equation (1) and (2) are used to calculate the total positive score (TotalPosScore) and total negative score (TotalNegScore), where n is the number of terms, and t denotes the tweet [16].

$$TotalPosScore_t = \sum_{s=1}^{n} TotalPosScore + PosScore_s \quad (1)$$

$$TotalNegScore_t = \sum_{s=1}^{n} TotalNegScore + NegScore_s \quad (2)$$

As given in Equation (3) sentiment polarity ($Polarity_{sa}(t)$) of a tweet can be a negative value, neutral (0) or a positive value [16]. The sentiment polarity is calculated for each of the tweets.

Fig. 4 demonstrates the frequency distribution of top 50 tokens from a typical download of 10,700 tweets. Positive terms such as “masumiyet” and “güzel” appear frequently in tweets. Series names and artist names are also frequently observed.

E. Algorithms

The classifiers were trained using pre-labeled Twitter data to precisely label the moods associated with the text, thus achieving the highest possible accuracy. We split the dataset as training and test sets by the ratio of 80% and 20%. Some of the classifiers have a tendency to cause overfitting by learning the detail and noise in the training dataset and show worse performance on a new dataset. We used 10-fold cross-validation to prevent the overfitting of classifiers.

Naïve Bayes, SVM, Random Forest algorithms, Bagging and Voting ensemble learning techniques were selected as machine learning algorithms. While the "sklearn" library in Python was used for machine learning algorithms, the "zeyrek" and "jype" libraries were used for zemberek.

Sklearn.svm library allows us to change the cost kernel and gamma values for the SVM algorithm. In the sklearn.model_selection library, parameters such as max depth in the tree, estimators, and maximum feature were set to the best estimator in the RF algorithm and run with maximum efficiency.

F. User Interface

In the scope of this study, a web-based user interface was designed for an easy and effective user experience. Users can display the general emotion distribution of current movies and TV series graphically and statistically on a dashboard. Another page was designed to monitor the most popular hashtags. Users can see the top hashtags and how many tweets related to a specific hashtag have been posted. A hashtag search page was supplied for the users to get more information about the hashtags they were interested in. By using the user interface given in Fig. 5, users can get details of hashtags they searched. On this page, the user can access the sentiment analysis results of the tweets, the username of the users who post the tweets, and the number of followers. The user can also view statistically how many positive, negative, or neutral tweets are related to the hashtag.

$$Polarity_{sa}(t) = \begin{cases} Positive\ or\ 1, if\ TotalPosScore(t) > TotalNegScore(t) \\ Negative\ or\ -1, if\ TotalPosScore(t) < TotalNegScore(t) \\ Neutral\ or\ 0, otherwise \end{cases} \quad (3)$$

TABLE II. EXAMPLE OUTPUT OF SENTIMENT ANALYSIS

Tokens	Total PosScore	Total NegScore	Sentiment Polarity
[‘Hülya’, ‘Avşar’, ‘a’, ‘seda’, ‘sayan’, ‘instagram’, ‘filtresi’, ’yap’, ’bakma’]	0.082781	0.916643	Negative
[‘grup’, ‘kucaklaş’, ‘ilker’, ‘masumiyet’, ‘harika’]	0.779853	0.050602	Positive
[‘mehdi’, ‘son’, ‘bölüm’, ‘allah’, ‘biz’, ‘sabır’, ‘ver’, ‘yolunsonu’]	0.039630	0.532317	Negative

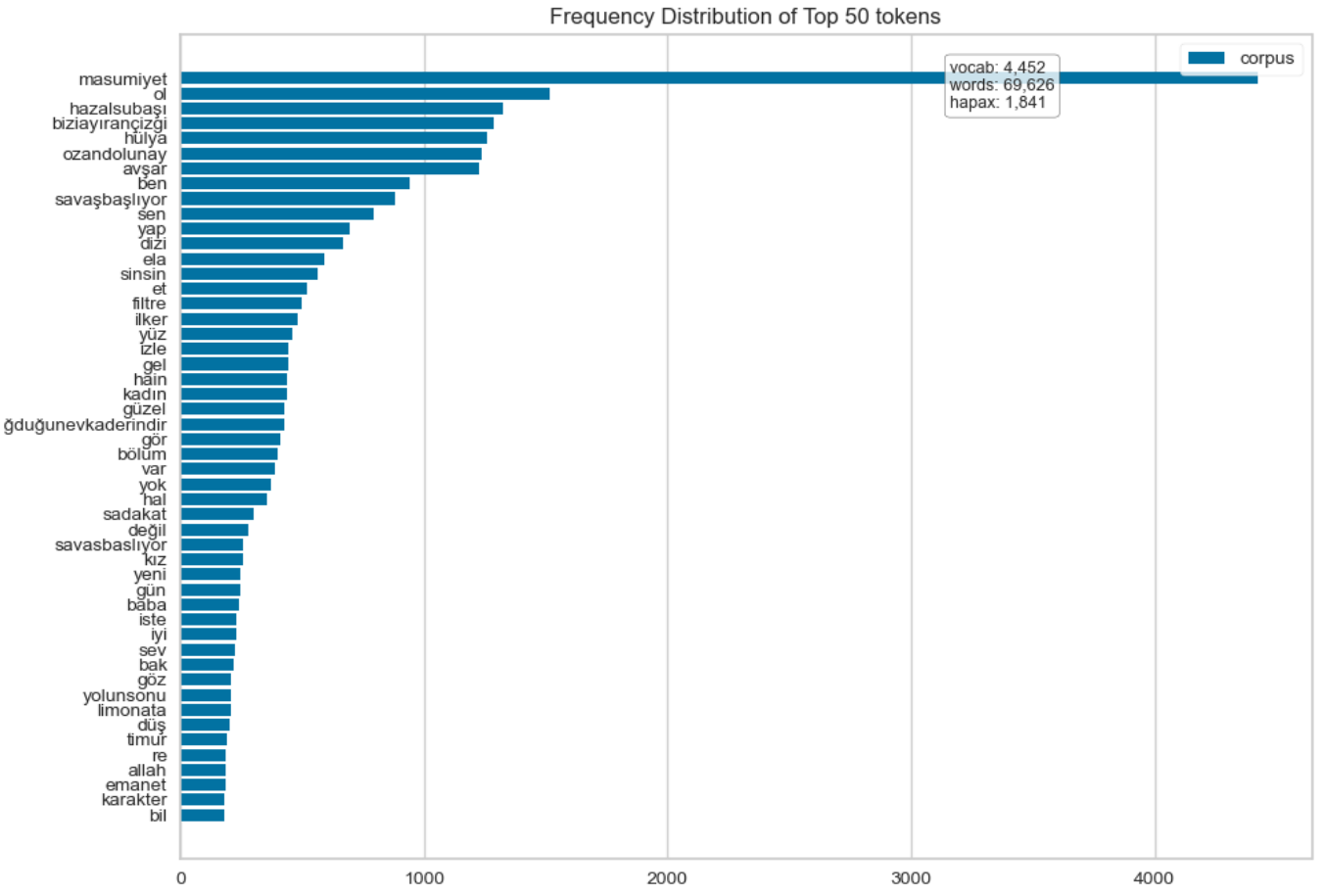

Fig. 4. Frequency distribution of top 50 tokens

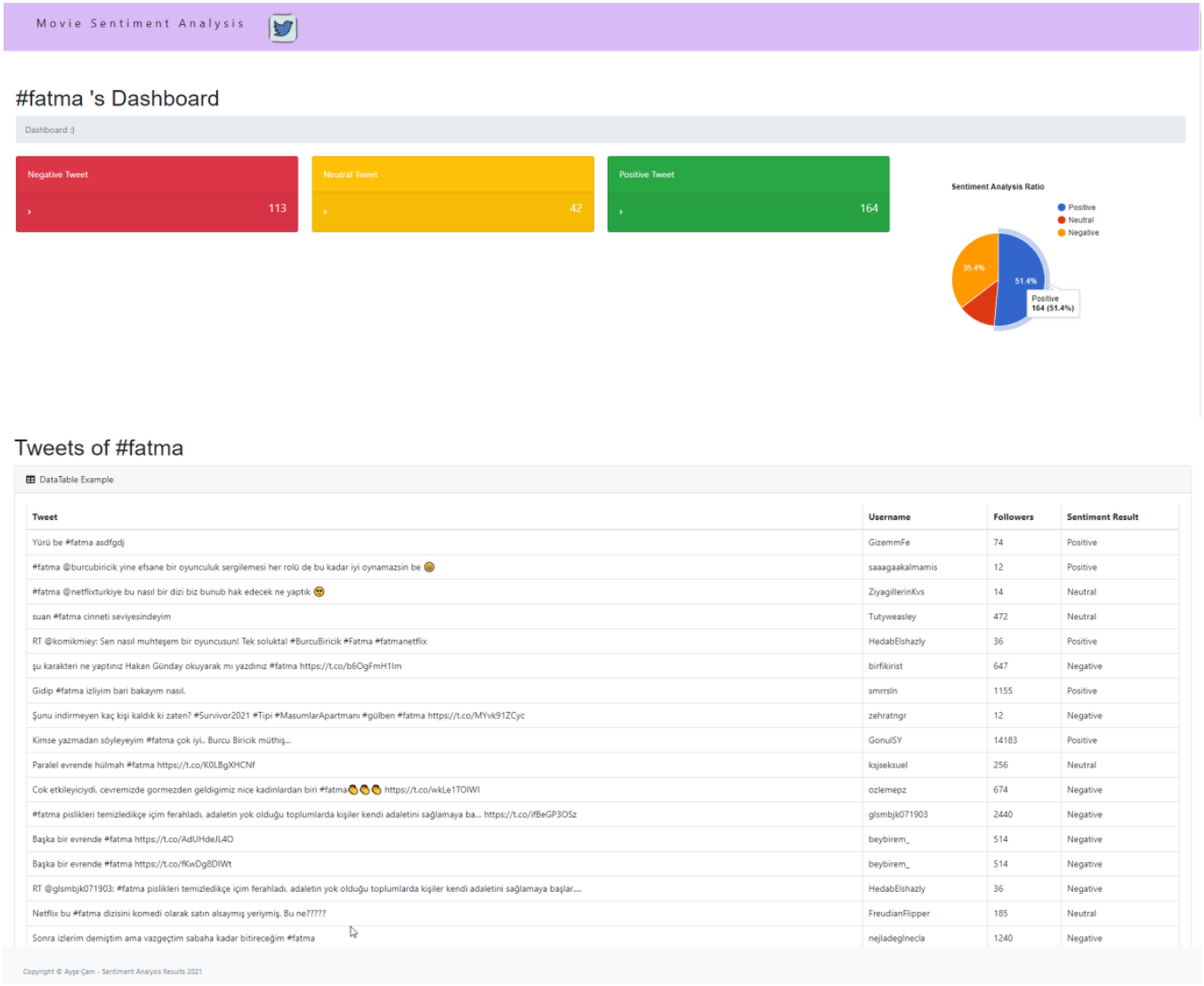

Fig. 5. Tweet-based and overall sentiment results for the hashtag #fatma.

IV. RESULTS

We labeled the tweets automatically by using BERT model and obtained 7,606 positive, 5,319 neutral, and 6,075 negative-labeled reviews. Machine learning algorithms have a tendency to ignore the minority class. We used an over-sampling method to avoid this problem. Naïve Bayes, SVM, random forest, and Voting and Bagging machine learning techniques are the techniques used to train the dataset and each technique creates slight differences in the result. These techniques are the well-known techniques used in sentiment analysis.

In the dataset, 80% of the data is used for training and the remaining (20%) for testing. Performance results of different techniques are given in Table 3 where 10-fold cross-validation technique is used to get realistic results. Parameter tuning was applied for each classifier and the best performance of each was obtained.

The Voting and SVM algorithms seem to give the best AUC values as 0.962 and 0.963, respectively. The best accuracy was obtained by the Voting algorithm as 87%. We obtained more accurate prediction results by combining lexicon-based and machine learning methods.

TABLE III. PERFORMANCE RESULTS FOR SENTIMENT ANALYSIS

	Precision	**Recall**	**Accuracy**	**F-Measure**	**AUC**
SVM	0.88	**0.86**	**86%**	**0.86**	**0.963**
Naïve Bayes	0.86	0.82	85%	0.83	0.950
Bagging	0.88	0.81	85%	0.83	0.959
Voting	**0.89**	0.83	87%	**0.86**	0.962
RF	0.87	**0.86**	**86%**	**0.86**	0.954

There are a few studies that deal with the sentiment prediction of text in the Turkish language. Atan and Çınar made dictionary-based emotion scoring and reached a correlation value of 0.79 between the emotional tones of the news and the market value of the companies [9]. In another study, Karagöz and Gürsoy, took the tweets written about the programs broadcast on a television channel over an eight-month period as a data set. By using semi-supervised technique, they created two separate dictionaries with positive and negative words and reached 68% accuracy by looking at the positive and negative excess with the help of excel.

The most obvious difference of this study from the existing studies on Turkish is the automatic labeling of tweets according to their sentiments. While the text data in other studies were labeled with the help of humans, the unlabeled data were first labeled with the Bert model, and then the success rate was increased up to 87% by using n-grams and using more than one machine learning algorithm in this study. When compared with the existing sentiment analysis studies performed on Turkish texts, our study has a promising performance.

V. CONCLUSION

In this study, emotion analysis was performed on the linguistic tweet dataset that contains comments about Turkish TV series and movies. The first step after collecting the tweets was cleaning the noise and removing outliers. By pruning and shaping the data, the data became a smaller and well-been dataset. Sentiment scores were calculated using Word stemming, lemmatization, and n-gram techniques. Tweets were tagged automatically using the Bert-based model according to their content. TF-IDF feature matrix was constructed using bigrams and unigrams and textual data was prepared for machine learning.

Machine learning algorithms including Naïve Bayes, SVM, Random Forest, Voting, Bagging were used to classify tweets as positive, neutral, or negative sentiment, and the performance of classifiers was measured for the accuracy and reliability of the classification models. Although all the classifiers performed well on the prepared dataset, when we handle the AUC metrics, SVM was the best classifier with the 0.963 AUC. Voting was the other successful classifier with 87% accuracy.

Consequently, in this study, a model that made more accurate predictions with SVM and Voting algorithms was created, and the emotional states of the audience of TV series and movies were displayed by the developed user interface.

REFERENCES

[1] S. Tuzcu, "Çevrimiçi Kullanıcı Yorumlarının Duygu Analizi ile Sınıflandırılması," *Eskişehir Türk Dünyası Uygulama ve Araştırma Merkezi Bilişim Dergisi*, 1(2), 1-5, 2020.

[2] D. Zimbra, A. Abbasi, D. Zeng, and H. Chen, "The state-of-the-art in Twitter sentiment analysis: A review and benchmark evaluation," *ACM Transactions on Management Information Systems (TMIS)* 9.2, 2018, 1-29.

[3] H. Wang, D. Can, A. Kazemzadeh, F. Bar, and S. Narayanan, "A system for real-time Twitter sentiment analysis of 2012 us presidential election cycle," *In Proceedings of the ACL 2012 system demonstrations*, pp. 115-120, July 2012.

[4] G. Abalı, E. Karaarslan, A. Hürriyetoğlu, and F. Dalkılıç, "Detecting citizen problems and their locations using twitter data,"*In Proceedings of the 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG)*, 2018, pp. 30-33, doi: 10.1109/SGCF.2018.8408936.

[5] K. Chakraborty, S. Bhatia, S. Bhattacharyya, J. Platos, R. Bag, and A. E. Hassanien, "Sentiment Analysis of COVID-19 tweets by Deep Learning Classifiers—A study to show how popularity is affecting accuracy in social media," *Applied Soft Computing*, 97, 106754, 2020.

[6] D. R. Pant, P. Neupane, A. Poudel, A. K. Pokhrel, and B. K. Lama, "Recurrent neural network based bitcoin price prediction by twitter sentiment analysis," *In Proceedings of the IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)*, pp. 128-132, October 2018.

[7] S. E. Shukri, R. I. Yaghi, I. Aljarah, and H. Alsawalqah, "Twitter sentiment analysis: A case study in the automotive industry" *In Proceedings of the IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT), IEEE*, pp. 1-5, November 2015.

[8] C. Quan and F. Ren, "Unsupervised product feature extraction for feature-oriented opinion determination," *Information Sciences*, 272, 16-28, 2014.

[9] S. Atan and Y. Çınar, "Borsa İstanbul'da finansal haberler ile piyasa değeri ilişkisinin metin madenciliği ve duygu (sentiment) analizi ile incelenmesi," *Ankara Üniversitesi SBF Dergisi*, 74.1, pp. 1-34, 2019.

[10] B. Karagöz and U. T. Gürsoy, "Adaptif Öğrenme Sözlüğü Temelli Duygu Analiz Algoritması Önerisi," *International Journal of Informatics Technologies*, 11(3), pp. 245-253, 2018.

[11] B. Pang, L. Lee, and S. Vaithyanathan, "Thumbs up? Sentiment classification using machine learning techniques," *arXiv preprint*, cs/0205070, 2002.

[12] R. Li, K. H. Lei, R. Khadiwala, and K. C. C. Chang, "Tedas: A twitter-based event detection and analysis system," *In Proceedings of the IEEE 28th International Conference on Data Engineering*, pp. 1273-1276, April 2012.

[13] M.E. Basiri, S. Nemati, M. Abdar, S. Asadi, and U.R. Acharrya, "A novel fusion-based deep learning model for sentiment analysis of COVID-19 tweets,"*Knowledge-Based Systems*, 228 (2021): 107242.

[14] M. J. D. Torres, "Contributions to Social Learning Analytics based on Sentiment Analysis of Students Interactions in Educational Environments," Doctoral dissertation, Universidad De Las Américas Puebla, 2019.

[15] O. Kaynar, Y. Görmez, M. Yıldız, and A. Albayrak, "Makine öğrenmesi yöntemleri ile duygu analizi," *In Proceedings of the International Artificial Intelligence and Data Processing Symposium*, pp. 17-18, 2016.

[16] R. Patel and K. Passi, "Sentiment analysis on Twitter data of world cup soccer tournament using machine learning," *IoT*, 1(2), pp. 218-239, 2020.

[17] MongoDB (2021, December 18), Retrieved from https://www.mongodb.com/.

[18] J. Devlin, M. W. Chang, K. Lee, and K. Toutanova, "Bert: Pre-training of deep bidirectional transformers for language understanding," *arXiv preprint arXiv:1810.04805*, 2018.

Journal of Emerging Computer Technologies
Research Article
Received: *2021-12-03* | ***Reviewing:*** *2021-12-03* & *2021-12-28* | ***Accepted:*** *2021-12-28* | ***Online:*** *2021-12-28* | ***Issue Date:*** *2021-12-31*

A Dynamic Method and Program for Multiple Password Generation and Management

Onur Çakırgöz
Department of Computer Engineering
Bartın University, Bartın, Turkey
onurcakirgoz@bartin.edu.tr
0000-0002-9347-1105

Süleyman Sevinç
Labenko Bilişim A.Ş.
İzmir, Turkey
suleysevinc@gmail.com
0000-0001-9052-5836

***Abstract*— Authentication is a process that should be fulfilled by users to gain access to websites/services. Today, the most common method used for authentication is still text-based passwords. However, several difficulties/problems are encountered during the use of passwords for authentication. One of them is that users must use a separate and strong password for each different website. Unfortunately, rather than using distinct passwords, users generally prefer to use the same password or similar passwords for different services, which inevitably leads to security vulnerabilities. Therefore, there is a need for a method/program that will enable easy and secure management of many strong passwords. In this study, a dynamic method and program is proposed to solve this problem. This method and program, inspired by the Chinese Remainders Theorem (CRT), simplifies the generation and management of multiple passwords. With this program, many individual passwords can be generated from a single unique password. Both the unique password and the individual passwords are not stored anywhere. The only thing users need to remember is the unique password, and in our method, long but easy-to-remember unique passwords can be used safely. Although inspired by the CRT, our method is not based on the CRT. CRT is only used in the security analysis of our method.**

Keywords*— *password, password management, password generation, chinese remainder theorem, authentication

I. INTRODUCTION

Since text-based password is economical and relatively easy to use, it is still the most widely used authentication method for electronic services [1], [2]. Besides, the number of websites that users visit to receive service, and in parallel, the number of passwords that they need to use are increasing day by day [1]. However, the password usage that increases in daily life has some consequences. The more passwords users have, the harder they are to remember. Also, since non-random and weak passwords are known to be prone to dictionary attacks, companies and institutions define policies/constraints on the password's strength [3]. The definition of some constraints by service providers upon the strength(predictability) of passwords, significantly increases the mental burden of the users [4]. From this point of view, many studies were conducted investigating password habits/behaviors of users [1], [2], [5], [6], [7], [8]. These studies showed that a significant portion of users, even some experts, use very similar passwords for different services, or even the same password. On the other hand, the password setting patterns of the users are also very similar. For example, most of the users use capital letters at the beginning of passwords, and numbers and punctuation at the end of passwords. Thus, particular service provider's security policies that are applied to the user passwords encounter the threat of losing the effects. In the worst-case, when a user uses same password for n different services, a malicious server/person can impersonate him/her and have illegal access to these n services.

Among the approaches that facilitate the use/management of passwords, password managers and password generators are the two prominent approaches. Password managers are applications that store user passwords in a place (locally or in a remote location) and retrieve passwords when requested. Most web browsers we use today also have this feature. Password generators, on the other hand, are applications that generate strong (hard to remember and guess) and random passwords and regenerate them when needed. The basic approach used by the majority of password generators is as follows: Generating new passwords by blending several pieces of information with a mathematical method. From this perspective, the two things that make the difference between password generators are the mathematical method used and the types of information blended. The password generator called *Site-Specific Passwords (SSP)* [9] is probably one of the oldest proposed solutions. The SSP creates a password by combining a user master password and an easy-to-memorize name that the user specifies for the website. The main problem with this approach is that as the number of websites increases, the user is likely to forget the names he/she set (especially for rarely used websites). The password generator named *Password Multiplier* [10] creates a password by combining the user master password, the website name, and the username for the website. *PasswordSitter* [11] generates a password as a function of the following components: user master password, user ID, website/service name, and some configurable parameters. The *Passpet* [12] application generates a password as a function of the user's master password and the name-icon pair selected by the user for the website. *ObPwd* [13] generates a password using two mandatory components (user master password and a website-specific object selected by the user) and one optional component (URL). *PALPAS* [14], unlike previous solutions, uses server-provided password policy data to generate passwords that meet the website's requirements. Password policy data is a small file created with a simple XML-based language. The other two components that *PALPAS* uses to generate the password are a stored master password and a client-side secret that is synchronized across all user devices. On the other hand, *AutoPass* [15] is a solution similar to *PALPAS* in terms of architecture and method. *AutoPass* fixed some of the shortcomings/problems of the previously proposed password generators. The Autopass client, which is an add-on to the web browser, communicates with the Autopass server. In case of Autopass server crash, the user cannot access (generate) passwords. Abderrahim Abdellaoui et al. proposed a scheme that performs authentication in a cloud environment [16]. The proposed scheme is based on a password generator that uses/blends methods such as multi-

Cite (APA): Cakirgoz, O., Sevinc, S. (2021). A Dynamic Method and Program for Multiple Password Generation and Management. *Journal of Emerging Computer Technologies*, 1(2), 61-67.
Volume:1, **No:**2, **Year:** 2021, **Pages:**61-67, December 2021, Journal of Emerging Computer Technologies

factor authentication, one-time password, and SHA1. Finally, drPass [17] is a protocol that helps users create and maintain different passwords for each web site. For drPass to be used, websites must accept this protocol and change their architecture accordingly.

There are also password generators developed as add-ons to various web browsers or as mobile applications. For example, *RndPhrase* (https://rndphrase.appspot.com) is a Firefox extension and similarly generates passwords as a function of some information. *PwdHash port* (https://addons.opera.com/en-gb/extensions/details/pwdhash-port) is an Opera extension and based on the *PwdHash* [18] password generator. On the other hand, *Password generator* (https://goo.gl/SNVtJY) is an Android application and generates passwords using configurable information.

Password managers are applications that help users to store and manage multiple passwords. Password manager programs are based on the basic principle of storing all user passwords (in encrypted form) in one place (usually locally). The user can access all the passwords stored locally with a unique password called the master key, which the user must know by heart. Among the current password management programs, *LastPass* (https://www.lastpass.com), *KeePass* (https://keepass.info), *Dashlane* (https://www.dashlane.com) and *1Password* (https://1password.com) stand out. When these four password manager programs are examined, it is seen that they all have the ability to automatically generate strong passwords depending on the user's request. From this point of view, these password managers also have a password generator feature. In addition, these four programs encrypt the database holding individual passwords with the AES-256 encryption algorithm. Most current online password managers learn or store account passwords and/or master passwords. In a recent study, this security vulnerability was addressed and *HIPPO* [19], a cloud-based password manager protocol that does not learn or store master passwords and account passwords, was proposed for the design of online password managers.

Single sign-on (SSO) protocols offer the opportunity to automatically share identity/authentication data between different sites [20], [21]. In this approach, a user authenticates only once and thus gains access to different web sites without having to re-authenticate. However, for this, SSO protocols require involved parties to first establish a circle of trust. Unfortunately, each service/site has different security requirements/levels and it's impossible to create a single unique federation where all parties trust each other [22]. Therefore, since there is no single unique SSO federation, the SSO approach is not able to provide a definite solution to the problem of managing the large number of passwords users have [23].

CRT is an ancient theorem which is frequently used in number theory, and it was originated by a Chinese mathematician Sun Tzu. To date, CRT was used in many scientific studies in both mathematics and computer science fields for different purposes. One of the earliest and well-known studies in computer science using the CRT is the (t,n) threshold scheme [24] proposed by Asmuth & Bloom. In 2007, S. Iftene presented a multi-authority e-voting scheme based on CRT [25]. J. C. Patra et al. proposed a novel CRT-based technique for digital watermarking in 2010 [26]. One year later, S. K. Kim et al. proposed new modular exponentiation and CRT recombination algorithms secure against all known power and fault attacks [27]. In 2014, K. Kaya, and A. A. Selçuk proposed a new threshold scheme for the Digital Signature Standard (DSS) using Asmuth–Bloom secret sharing based on the CRT [28]. There are also many recent studies in the literature that use the CRT for different purposes such as secret sharing [29], image sharing [30], key agreement [31], data encryption [32] and data compression [33].

Due to security requirements, users must use a separate and strong (cannot be guessed easily and hard to remember) password for each different website. It is nearly impossible for users to memorize/remember large numbers of strong passwords. Therefore, there is a need for a method/program that will enable easy and secure management of large numbers of passwords. In this study, a dynamic method and program is proposed for this need. The sections of the article are as follows: In the second section, firstly, it is mentioned about the passwords and the conversion of passwords into a numeric value with polynomial representation, then, the CRT is introduced, its formulas are given, and finally, the method and program we developed for the generation and management of multiple passwords are explained. In the third chapter, sample individual passwords produced by our program are shown, and the properties and security of our method is discussed. Final remarks are given in the last section.

II. CHINESE REMAINDER THEOREM

CRT is about finding a solution to the system of simultaneous congruences. Suppose that X, a and p are positive integers. Then, (1) defines a congruence.

$$X \equiv a(mod\ p) \tag{1}$$

A system of simultaneous congruences is defined in (2). Here $p_1,p_2,...,p_n$ should be pairwise coprimes. Namely, greatest common divisor; $gcd(p_i, p_j)$ should be 1 for all $1 \leq i,j \leq n$ and $i \neq j$. Then, this system of simultaneous congruences has a unique solution X (mod r).

$$X \equiv a_i\ (mod\ p_i)\ (i = 1,2,\cdots,n) \tag{2}$$

Given,

$$r = \prod_{i=1}^{n} p_i \tag{3}$$

Let,

$$M_i = \prod_{j=1, j\neq i}^{n} p_j\ \ (i = 1,2,\cdots,n) \tag{4}$$

Then, unique solution *X* is computed as in (5):

$$X = (\sum_{i=1}^{n} a_i M_i (M_i{}^{-1} mod\ p_i))\ (mod\ r) \tag{5}$$

III. THE DYNAMIC METHOD AND PROGRAM FOR MULTIPLE PASSWORD GENERATION AND MANAGEMENT

For the generation and management of multiple passwords, firstly, a method called the backward direction method was developed. In fact, the backward direction method is exactly based on the CRT. Unfortunately, as a result of the evaluations, it was seen that the method contains some

problems, and it is not possible to use it. Then, a different method, called forward direction method, was developed. The forward direction method is not based on the CRT. The CRT was only evaluated in the security analysis of this method. Both methods were described in detail below.

A. Backward Direction Method

Based on CRT, we might think (a_1, a_2, ..., a_n) in (2) as n individual passwords (we already have or to be generated). In response to these, prime numbers (p_1, p_2, ..., p_n) that are greater than these numbers can be generated randomly and can be used to acquire individual passwords. The solution of this system of simultaneous congruences would give us the X, namely, the unique password.

Extracting individual passwords from X is straightforward. In this case, k'th individual password can be computed as $X \equiv a_k \pmod{p_k}$.

Then, what we need to obtain individual passwords are the value of X and the corresponding prime numbers. When X and the respective prime number are put together, the desired individual password can be easily acquired. But, having them individually is not sufficient to obtain the password. In the light of this information, we can define the required steps for backward direction method:

1) Convert each of the n passwords to integer by using Horner method.

2) For each password, generate a prime number that is greater than password and distinct from each other.

3) Compute the unique password X from the equation system.

4) Store prime numbers in a file. Also, remove n passwords.

The "Backward_Direction_Method()" algorithm generates unique password X and prime numbers in accordance with the backward direction method:

```
Backward_Direction_Method(string[] passwords)
01  n = passwords.Length
02  Let Num_psw[0..(n+1)] be a new Biginteger array
03  for i = 0 to n-1
04      Num_psw[i] =
Convert_String_to_Integer(passwords[i])
05  for j = n to (n+1)
06      number = Randomly generate a Biginteger value
07      Num_psw[j] = number
08  Let primes[0..(n+1)], Mi_values[0..(n+1)] and
I_o_Mi[0..(n+1)] be new Biginteger arrays
09  primes = Find_primes_for_passwords(Num_psw, n+2)
10  Mi_values = Find_Mi_Values(primes)
11  M_value = Find_M_Value(primes)
12  I_o_Mi = Return_inverse_of_Mi(Mi_values, primes)
13  X_value = Compute_X(Num_psw, Mi_values, I_o_Mi,
primes, M_value)
14  X = Convert_Integer_to_String(X_value)
15  Print X to the screen, store first n primes in a file
```

In order to increase the security of the backward direction method, two extra pairs of passwords and prime numbers are created in the algorithm, and these are included in the solution set. However, extra generated passwords and prime numbers are discarded and are not shown to the user. The reason for generating two extra password-prime number pairs is to prevent a malicious person from finding the unique password by obtaining some or all of the password-prime number pairs of the user.

The details and working logic of the algorithm are as follows: The "passwords" parameter is a string array, and it holds individual passwords. In line 1, the number of individual passwords is assigned to the "n" variable. The "Num_psw" array is defined in Line 2, and this is used to hold numerical equivalents of individual passwords. There is a for loop in Lines 3 and 4, and the numerical equivalents of all individual passwords are assigned to the first n elements of the "Num_psw" array. Similary, there is a for loop between Lines 5 and 7, and randomly generated two biginteger values are assigned to the last 2 elements of the "Num_psw" array. In line 8, "primes", "Mi_values" and "I_o_Mi" arrays are defined, and they hold prime numbers, M_i values in (4), and inverse of M_i values (M_i^{-1}) in (5), respectively. In line 9, prime numbers are generated randomly by the "Find_primes_for_passwords()" method and they are assigned to the "primes" array. In line 10, M_i values are calculated by the "Find_Mi_Values()" method, which corresponds to (4), and then, they are assigned to "Mi_values" array. In line 11, M value (r in (3)) is calculated by the "Find_M_Value()" method, which corresponds to (3), and then, it is assigned to "M_value" variable. In line 12, inverses of M_i values (M_i^{-1}) calculated by the "Return_inverse_of_Mi()" method are assigned to "I_o_Mi" array. In line 13, the integer equivalent of the master password is calculated by the "Compute_X()" method, which corresponds to (5), and then, it is assigned to "X_value" variable. In line 14, the unique (master) password is obtained by converting the integer stored in "X_value" variable to string. Finally, in line 15, the master password is shown on the screen and the first n primes are stored in a file.

The password generation page in backward direction method is shown in Fig. 1. The user can easily generate the master (unique) password by entering individual passwords via the form in Fig. 1.

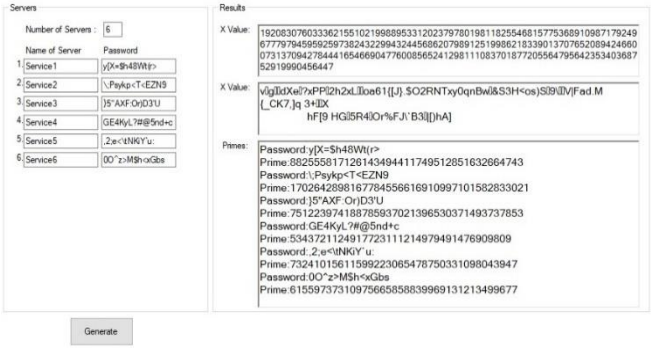

Fig. 1. Password generation page in backward direction method

On the form, user first specifies the number of servers. After that, equal number of textboxes for the names of the servers and for the passwords become visible on the page. Then, user fills the textboxes. Finally, when user clicks on the Generate button, program runs pre-defined methods, writes the names of the server to a text file and prints out unique password, numerical equivalent of unique password, and prime numbers. Furthermore, numeric values of individual passwords, Mi values, inverse of Mi values and M value are printed out. As seen in the figure, the generated unique password X is not a memorable password.

As mentioned previously, users define either similar passwords or same password for different service providers. Obviously, this is a significant security problem. Since individual passwords in backward direction method are defined by the users in advance, the backward direction method does not yield a solution to this security problem. Furthermore, backward direction method has three important drawbacks:

1) The generated X is a very big integer, and the string equivalent of X is not a memorable password. In addition, there are some white-space or control characters in the unique password produced. (As is known, the first 32 characters in ASCII table are not printable - they are control characters.)

2) New passwords cannot be added to the solution system later. Because, when a new individual password and the corresponding prime number are included in the solution system, the unique password changes automatically.

3) As the number of individual password-prime pairs in the equation system increases, the length of the unique password automatically increases.

Due to these three important problems, the backward direction method cannot be used by users in practice. In order to overcome the second problem of the backward direction method (not being able to add new individual passwords to existing individual passwords later), a random prime number (p_i) can be generated first, and then a new individual password can be obtained with X % p_i operation. (This solution approach, with some differences, already corresponds to the basic logic of the forward direction method, which will be explained in the next section.)

B. Forward Direction Method

Instead of starting from the individual passwords, users can first determine the unique password X, which is sufficiently complex but memorable. Secondly, sufficiently large n numbers (divisors) are generated randomly. Here, n numbers should not be pairwise coprime for security reasons. Then, individual passwords can be obtained via the equation (X mod p_k) (for the k'th service). Accordingly, the steps of the forward direction method can be defined as following:

1) Determine a strong unique password X.

2) Convert X into its numerical equivalent with Horner method.

3) Generate n random and distinct integers (divisors) which are not pairwise coprimes.

4) Perform (X mod p_i) for p_1, p_2, ..., p_n. (Here, p_i representation is used for divisors, as well)

5) Convert the results after modulo operation to their string equivalents. Use the results after conversion as individual passwords, but don't store them somewhere.

6) Store n divisors in a file.

The "Forward_Direction_Method()" algorithm generates individual passwords and divisors in accordance with the forward direction method. The details and working logic of the algorithm are as follows: The "password" parameter is the unique password. On the other hand, the "number" parameter shows the number of individual passwords (and naturally, the number of divisors) to be generated. In line 1, the integer equivalent of the unique password is calculated, and this value is assigned to the variable "Xvalue". The "divisors" and "passwords" arrays are defined in line 2, and these arrays hold the divisors and individual passwords that will be presented to the user, respectively. There is a while loop between lines 4 and 11, and the two variables ("flag" and "index") defined in line 3 are used appropriately in this loop. In line 5, a divisor is generated randomly by the "Find_divisor_number()" method and this divisor is assigned to the "newdivisor" variable. ("newdivisor" is of type Biginteger.). In line 6, the individual password is obtained by converting the result of the operation (the numeric equivalent of the unique password % the divisor produced) to string, and the individual password is assigned to the variable "psw". In the if statement on the 7th line, it is checked whether the individual password meets the criteria/ restrictions (e.g., minimum-maximum or fixed length, the variety of symbols the password is required to contain, etc.) and whether the currently generated divisor is different from the previously generated ones. Here, since different constraints can be defined for each individual password, the "Control_password()" algorithm checks the individual password with password-specific constraints. Also, "Control_divisor()" algorithm in line 7 checks whether the currently generated divisor and the previously generated ones are pairwise coprimes. If the individual password and the divisor meet the criteria, they are recorded in the respective arrays. If the specified number of individual passwords are generated, the loop is terminated (Lines 11-12). Finally, in line 13, all divisors are stored in a file.

```
Forward_Direction_Method(string password , int number)
01  Xvalue = Convert_String_to_Integer(password)
02  Let divisors[0..number-1] be a new Biginteger array and
passwords[0..number-1] be a new string array
03  flag = true, index = 0
04  while(flag)
05     newdivisor = Find_divisor_number()
06     psw = Convert_Integer_to_String(Xvalue %
newdivisor)
07     if (Control_password(psw) &&
Control_divisor(divisors, newdivisor))
08          divisors[index] = newdivisor
09          passwords[index] = psw
10     index = index + 1
11     if (index = = number)
12          flag = false
13  Store divisors in a file
```

The password generation page in forward direction method is shown in Fig. 2. The user can easily generate individual passwords by entering the unique password via the form in Fig. 2. The details are as follows: If the user clicks on the Calculate button after entering the unique password and the number of passwords to be generated, the program asks for the properties (restrictions) of each individual password. After this stage, the program executes predefined methods and shows the generated passwords and divisors on the screen. As a general constraint, the generated individual passwords consist of only keyboard characters. This is provided via a simple function ("Control_password()") which checks the generated passwords. If the numerical equivalents of the characters constituting a password is between [33..125] in the ASCII table, this string is accepted as a password.

The divisors required to obtain individual passwords are stored in a simple text file together with the server names. An example text file generated by the program and that holds divisors is seen in Fig. 3. In this way, all individual passwords

can be obtained easily by entering the unique password to the program. At this point, the operations of the program are quite simple: reading the file that holds the divisors and performing the modulo operations.

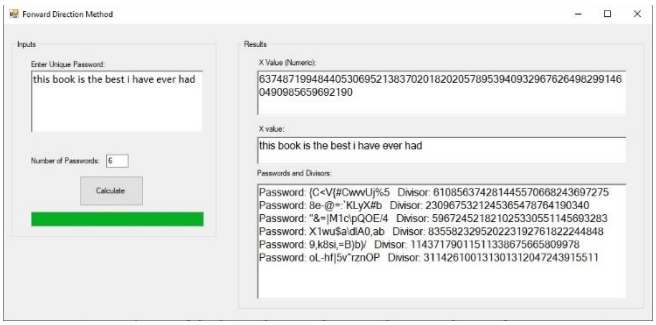

Fig. 2. Password generation page in forward direction method

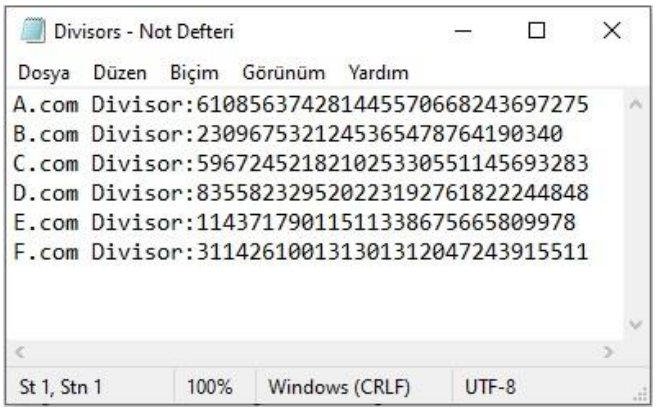

Fig. 3. The text file generated by the program and that holds divisors

IV. RESULTS AND DISCUSSION

The number of all possible passwords that can be generated in the forward direction method and the properties of the passwords depend on many parameters. These parameters can be listed as follows:

- Size of symbol space
- Unique password defined by the user
- Minimum character length constraint defined on the unique password
- Divisors randomly generated by the program
- Minimum value constraint defined on divisors
- Various constraints on the individual passwords to be generated (minimum character length, the variety of symbols the password is required to contain)

On the other hand, in order to provide the minimum character length constraint defined on individual passwords, randomly generated divisors must also be larger than the numerical equivalents of individual passwords. The parameter values determined in the developed application and the constraints defined for passwords are given in Table-1. Based on these parameter values and defined constraints, nearly 93^{13} different individual passwords which consist of 13 characters can be generated. The relevant constraints given in Table-1 were applied to all individual passwords to be generated. That is, the same constraints were defined for all individual passwords. In accordance with the parameter values and constraints specified in Table-1, sample individual passwords, divisor numbers and numerical equivalents of passwords produced by the application are given in Table-2. In Table-2, the divisor numbers used to generate individual passwords range from 28 to 30 digits. Similarly, the numerical equivalents of individual passwords range from 27 to 30 digits. On the other hand, in this example, "this book is the best i have ever had" is chosen as the master password. This is a very easy phrase to memorize and remember.

TABLE I. PARAMETER VALUES IN THE APPLICATION AND CONSTRAINTS DEFINED FOR PASSWORDS

Parameter/Constraint	Value
The Length of Symbol Space(s)	93 (keyboard characters whose decimal values are between 33 and 125 in the ASCII table)
The minimum Length of Unique Password	30
The minimum Length of Individual Passwords	13
Other Constraints Defined for Individual Passwords	Must contain at least one uppercase letter, at least one lowercase letter, at least one number, and at least one punctuation mark.

TABLE II. SAMPLE INDIVIDUAL PASSWORDS GENERATED IN THE FORWARD DIRECTION METHOD AND OTHER ASSOCIATED DATA

Property	Value
Unique Password	this book is the best i have ever had
Numeric Equivalent of Unique Password	637487199484405306952138370201820205789539409329676264982991460490985659692190 (78 digits)
Number of Individual Passwords Generated	6
The Generated Individual Password and Divisor Pairs	Password1: {C<V{#CwvvUj%5 Numeric_value_of_Password1: 276201135629902806667468828515 (30 digits) Divisor1: 610856374281445570668243697275 (30 digits) Password2: 8e-@=:`KLyX#b Numeric_value_of_Password2: 999950350888928822060524610 (27 digits) Divisor2: 230967532124536547876419034 0 (28 digits) Password3: "&=|M1c\pQOE/4 Numeric_value_of_Password3: 766974946207805364219047752 92 (29 digits) Divisor3: 596724521821025330551145693283 (30 digits) Password4: X1wu$a\dlA0,ab Numeric_value_of_Password4: 197636672696185503159209650158 (30 digits) Divisor4: 835582329520223192761822244848 (30 digits) Password5: 9,k8si,=B)b)/ Numeric_value_of_Password5: 100972169686289301582957100 2 (28 digits) Divisor5: 114371790115113386756658099 78 (29 digits) Password6: oL-hf|5v^rznOP Numeric_value_of_Password6: 249526971213973380176697533304 (30 digits) Divisor6: 311426100131301312047243915511 (30 digits)

The CRT corresponds to the backward direction method, but the forward direction method is a different approach from the CRT. Our multiple password generation and management program is based on the forward direction method. One of the strong features of the method and the program is that both the unique password and individual passwords are not stored anywhere. Only the divisors needed to obtain individual passwords are kept in a file. The divisors do not mean anything on their own. Moreover, in the forward direction method, even the divisor-individual password pairs are not sufficient to find the unique password. Because, as the CRT states, all p_i's in (1) should be pairwise coprimes. However, in the forward direction method, the divisors are generated in such a way that they are not pairwise coprimes. Therefore, even though we have all the divisor-individual password pairs, it is not possible to find the unique password using the CRT.

As shown in Table-2, there is a huge difference (in terms of numerical size) between the numerical equivalent of the unique password and the divisors. In this example, the numerical equivalent of the unique password is 78 digits, whereas the largest divisor is 30 digits. Another meaning of this is that the quotient values are much larger than the divisor numbers during modulo operations. With a simple mathematical calculation, it can be found that the quotient values correspond to a number of at least 48 digits. On the other hand, today, an ordinary personal computer at 3 GHz can perform approximately $2.7x10^{14}$ transactions (for a single core of the processor) in 1 day. Even if the individual password and divisor pair are known, the time required to find the unique password using a brute force approach is nearly 10^{34} days.

V. CONCLUSION

In general, the number of websites where users register to get services is quite high, and this number is increasing day by day. Naturally, for security reasons, users must define and maintain strong and distinct passwords for these different websites. On the other hand, memorizing and bearing many strong passwords in mind is a difficult task. From this point of view, in this study, a dynamic method and program is proposed for the generation and management of many distinct and strong passwords. The proposed method is mainly based on modulo operation. In this method, the user first defines an easy-to-remember and relatively long unique (master) password. Then, the user can easily generate individual passwords by entering the program the unique password and the number of individual passwords he/she wants to generate. One of the most important features of our method is that the generated individual passwords are not stored anywhere. Only the divisors used to obtain individual passwords are stored in a simple text file. On the other hand, the characteristics of the generated individual passwords depend on many parameters. Individual passwords with desired properties can be generated by defining different constraints.

Since the equation system created by our method is similar to the CRT, the CRT was evaluated in the security analysis part of the method. Our approach does not introduce new risks for authentication. Without any loss of security, this approach has the potential to increase the usability of password-based authentication, and individual passwords created would not be prone to dictionary attacks. As a result, our multiple password generation and management program provides managing many individual passwords through a master password and makes password-based authentication more practical and easier to manage for users.

REFERENCES

[1] W. A. S. A. Alothman, "Evaluating Passwords User Behavior and the Psychology of Password Management", *International Journal of Engineering and Computer Science*, 8(04), 24586–24602, 2019.

[2] E. Stobert, R. Biddle, "The password life cycle", *ACM Transactions on Privacy and Security (TOPS)*, *21*(3), 1-32, 2018.

[3] P. Arias-Cabarcos, et. al., "Comparing password management software: toward usable and secure enterprise authentication", *IT Professional*, 18(5), 34-40, 2016.

[4] B. Brumen, "System-Assigned Passwords: The Disadvantages of the Strict Password Management Policies", *Informatica*, *31*(3), 459-479, 2020.

[5] Y. Y. Choong, "A cognitive-behavioral framework of user password management lifecycle", In International Conference on Human Aspects of Information Security, Privacy, and Trust, Springer, Cham, 127-137, June 2014.

[6] E. Stobert, R. Biddle, "Expert password management", In International Conference on Passwords, Springer, Cham, 3-20, December 2015.

[7] B. E. Ur, Supporting password-security decisions with data, PhD Thesis, Carnegie Mellon University, 2016.

[8] C. Shen, et. al., "User practice in password security: An empirical study of real-life passwords in the wild", *Computers & Security*, 61, 130-141, 2016.

[9] A. H. Karp, Site-specific passwords, HP Laboratories, Palo Alto, Tech. Rep., May 2003.

[10] J. A. Halderman, B. Waters, E. W. Felten, "A convenient method for securely managing passwords", In Proceedings of the 14th international conference on World Wide Web, 471-479, May 2005.

[11] R. Wolf, M. Schneider, The passwordsitter, Fraunhofer Institute for Secure Information Technology (SIT), Tech. Rep., May 2006.

[12] K. P. Yee, K. Sitaker, "Passpet: Convenient password management and phishing protection", In Proceedings of the second symposium on Usable privacy and security, 32-43, July 2006.

[13] M. Mannan, P. C. van Oorschot, "Passwords for both mobile and desktop computers: ObPwd for Firefox and Android", *USENIX ;login*, 37(4), 28–37, 2012.

[14] M. Horsch, A. Hülsing, J. A. Buchmann, "PALPAS — passwordless password synchronization", In 2015 10th International Conference on Availability, Reliability and Security, 30-39, August 2015.

[15] F. Al Maqbali, C. J. Mitchell, "AutoPass: An automatic password generator", In *2017 International Carnahan Conference on Security Technology (ICCST)*, 1-6, IEEE, October 2017.

[16] A. Abdellaoui, Y. I. Khamlichi, H. Chaoui, "A novel strong password generator for improving cloud authentication", *Procedia Computer Science*, *85*, 293-300, 2016.

[17] S. Panda, S. Mondal, "drPass: A Dynamic and Reusable Password Generator Protocol", In International Conference on Information Systems Security, 407-426, Springer, Cham, December 2018.

[18] B. Ross, et. al., "Stronger Password Authentication Using Browser Extensions", In USENIX Security Symposium, 17-32, August 2005.

[19] M. Shirvanian, et. al., "A hidden-password online password manager", In *Proceedings of the 36th Annual ACM Symposium on Applied Computing*, 1683-1686, March 2021.

[20] P. Arias-Cabarcos et al., "Blended Identity: Pervasive IdM for Continuous Authentication", *IEEE Security & Privacy*, 13(3), 32–39, 2015.

[21] F. Alaca, P. C. V. Oorschot, "Comparative analysis and framework evaluating web single sign-on systems", *ACM Computing Surveys (CSUR)*, *53*(5), 1-34, 2020.

[22] P. Arias-Cabarcos, et. al., "Comparing password management software: toward usable and secure enterprise authentication", *IT Professional*, *18*(5), 34-40, 2016.

[23] N. Katuk, et. al., "Can single sign-on improve password management? A focus group study", Pattern Analysis, Intelligent Security and the Internet of Things, Advances in Intelligent Systems and Computing, 85-93, Springer, Cham, 2015.

[24] C. Asmuth, J. Bloom, "A modular approach to key safeguarding", *IEEE transactions on information theory*, *29*(2), 208-210, 1983.

[25] S. Iftene, "General Secret Sharing Based on the Chinese Remainder Theorem with Applications in E-Voting", *Electronic Notes in Theoretical Computer Science (ENTCS)*, 186, 67–84, 2007.

[26] J. C. Patra, A. Karthik, C. Bornand, "A novel CRT-based watermarking technique for authentication of multimedia contents", *Digital Signal Processing*, 20, 442-453, 2010.

[27] S. K. Kim, et. al., "An efficient CRT-RSA algorithm secure against power and fault attacks", *The Journal of Systems and Software*, 84(10), 1660-1669, 2011.

[28] K. Kaya, A. A. Selçuk, "Sharing DSS by the Chinese Remainder Theorem", *Journal of Computational and Applied Mathematics*, 259, 495-502, 2014.

[29] Y. H. Chou, G. J. Zeng, X. Y. Chen, S. Y. Kuo, "Multiparty weighted threshold quantum secret sharing based on the Chinese remainder theorem to share quantum information", *Scientific Reports*, *11*(1), 1-10, 2021.

[30] K. Meng, F. Miao, Y. Xiong, C. C. Chang, "A reversible extended secret image sharing scheme based on Chinese remainder theorem", *Signal Processing: Image Communication*, *95*, 116221, 2021.

[31] Y. Jiang, Y. Shen, Q. Zhu, "A Lightweight Key Agreement Protocol Based on Chinese Remainder Theorem and ECDH for Smart Homes", *Sensors*, *20*(5), 1357, 2020.

[32] T. Duseja, M. Deshmukh, "Image compression and encryption using chinese remainder theorem", *Multimedia Tools and Applications*, *78*(12), 16727-16753, 2019.

[33] R. Vidhya, M. Brindha, "Evaluation and performance analysis of Chinese remainder theorem and its application to lossless image compression", *Journal of Ambient Intelligence and Humanized Computing*, 1-16, 2021.

Journal of Emerging Computer Technologies
Research Article
Received: *2021-10-22* | ***Reviewing:*** *2021-10-22* & *2022-01-07*| ***Accepted:*** *2022-01-07* | ***Online:*** *2022-01-08* | ***Issue Date:*** *2021-12-31*

Overview of Techniques and Methods for Stress Recognition

Natasa Koceska
Faculty of Computer Science,
University of Goce Delchev, "Krste Misirkov" 10-A,
Shtip, North Macedonia
natasa.koceska@ugd.edu.mk
0000-0002-3392-8871

Saso Koceski
Faculty of Computer Science,
University of Goce Delchev, "Krste Misirkov" 10-A,
Shtip, North Macedonia
saso.koceski@ugd.edu.mk
0000-0002-5513-1898

***Abstract*— Stress has become a significant cause of many diseases in modern society, such as high blood pressure, atherosclerosis, heart disease, obesity, diabetes, insomnia etc. Moreover, the Covid-19 pandemic negatively affects people's mental health, increasing depression and anxiety. This raised the question of whether automatic stress detection and recognition systems can be developed and used in everyday life. In this review study, we will examine the recent works on stress recognition systems by reviewing the techniques and methods used. Only studies involving human participants were taken into consideration, as no such analysis has been made so far. By providing a comprehensive review of the state-of-the-art, we would like to encourage other researchers to take active participation in the field of stress research as well as to explore the benefits and opportunities offered by stress recognition systems.**

Keywords— Stress recognition, stress detection, physiological, behavioural, multimodal, machine learning

I. INTRODUCTION

Stress can be defined as any type of change that causes physical, emotional, or psychological strain. When you experience changes or challenges (stressors), your body produces physical and mental responses. These stress responses help your body adjust to new situations. Under stress, the body is flooded by stress hormones including adrenaline and cortisol, which rouse the body for emergency action. The heart pounds faster, muscles tighten, blood pressure rises, the breath speeds up and senses become sharper.

Stress can be positive ("eustress"), keeping us alert, motivated and ready to avoid danger. This positive stress can improve the performance in everyday situations (e.g.: during a stage performance, during job presentation, during school exams, winning a race etc.). Stress becomes a problem (negative stress - "distress") when stressors continue without relief or relaxation between challenges. As a result, the person becomes overworked and creates stress-related tension, which affects their lifestyle.

Human body is well equipped to handle stress in small doses, but when that stress becomes long-term or chronic, it can have serious effects on the body. Evidence indicate that severe or prolonged (chronic) stress resulted in increased risk for physical and mental disorders, which is called stress-related disease. Stress is the common risk factor of 75%–90% diseases, including cardiovascular diseases, metabolic diseases, psychotic and neurodegenerative disorders, cancer etc. Thus, it is necessary to manage mental stress before it causes negative impacts on people. For the proper management, it should be beneficial to recognize whether individuals become stressed or not whenever they stand in the middle of stressful episodes. In addition, detecting and recognizing stress play a particularly important role in certain work environments.

Much progress has been done in the last years towards the development of an automatic stress recognition systems. Various approaches exist that involve the use of physiological signals (heart rate variability, hormone levels, electrocardiogram, etc.), behavioural responses (keystroke and mouse dynamics, posture, mobile phone usage, etc.), contextual events (place, time, ambient factors), and multi-modal techniques (combination of multiple type of data).

This work reviews and brings together the recent works carried out in the last 5 years, in the field of stress recognition. The stressors, techniques, results, advantages, limitations, and issues for each study are highlighted and expected to provide a path for future research studies.

II. METHODOLOGY

The approach adopted in this review firstly performs search through two databases: Science Direct and IEEE Xplore, with the search keywords: "stress recognition" OR "stress detection". Relevant papers were considered only papers published in last 5 (from 2016 till the end of 2020). This was considered appropriate due to the rapid technology development in this field.

The result of the query was a set of over 200 articles from both databases. After careful analysis (titles and abstracts of all papers were reviewed in order to retain only the relevant ones), and duplicate removal, 73 research papers from journals, conferences or early access articles, were selected for further reading. These articles were divided into two groups: articles where stress recognition is made using data from the existing databases, and articles where stress detection and classification is performed using the human participants.

After identifying the main modalities involved in the current state of stress recognition, it was decided in this review study to analyze only the second group of articles (with user participation), as no such analysis has been made so far. Thirty research papers were identified and included in the final analyses. Each one of the selected papers was fully read and specific information were extracted. The collected information is summarized in Table I.

III. REPORTING THE RESULTS

Selected papers were divided into two major groups: studies where stress recognition was done using physiological signals and studies where behavioural signals are used for stress recognition.

TABLE I. SUMMARY OF SELECTED PAPERS

Ref. Num	Parameters measured	Hardware (sensors) used during the measurement	Measuring environment	Stress induction	Algorithm	Results (accuracy)	Advantage/Disadvantage	Limitations
[1]	Heart rate , skin temperature, galvanic skin response of the hand, oxygen saturation, and breath-flow rate	E-Health V2 (Cooking Hacks, Spain) shield and the Arduino Uno board	Academic environment-laboratory settings	Neutral task, non-stress task (listening to instrumental music), and a stress task (time-constrained arithmetic task)	Support Vector Machine (SVM), k-Nearest Neighbors (KNN), Random Forest and Logistic Regression (LogR)	Two class stress: KNN - 95.98% anxiety: SVM - 98.89%	/	Only one type of stress task was tested
[2]	EEG	Wearable EEG sensor (Emotiv EPOC+)	3 construction sites	Job site stressors: working hazards and tiredness	k-Nearest Neighbors (k-NN); Gaussian Discriminant Analysis (GDA); Support Vector Machine (SVM)	80.32% - Gaussian SVM	Need of applying multi-subjects/tasks learning algorithms, which optimize classifier parameters for different tasks and subjects (on contrary of static ones applied)	/
[3]	Thermal images	FLIR SC7600 thermal IR imager (infrared camera), chest strap heart monitor (Garmin) and a finger probe (Miroxi) to measure HR	Laboratory settings	Heavy running, Trier Social Stress Test	Eulerian magnification-canonical correlation analysis (EM-CCA) Back propagation (BP) neural network	90%	More efficient and accurate thermal imaging tracking algorithm is required. Relationship between amplification intervals and different types of stress should be further refined, here it is based on blind source analysis	/
[4]	EMG, ECG	ECG v.12 Bayamed, Datalog Biometrics (EMG), SX230 surface electrode (EMG) and Skintact F-55 electrode (ECG)	Laboratory settings	Mental arithmetic, Stroop color-word test	SVM with RBF kernel	Two, three and four levels classification 100%, 97.6%, and 96.2%,	/	Lack of evaluation in real-world applications - recording EMG signals in an uncontrolled environment is challenging
[5]	Electrodermal activity (EDA), Electrocardiography (ECG), Electromyography (EMG), Reaction Time (RT)	BIOPAC System, Two LEDs (for RT measurement)	Laboratory settings	Visual stressor (Stroop test) and auditory stressor	SVM	Visual stressor – over 83.3% Auditory stressor – over 71.4%	/	/
[6]	EEG	Wired-EEG Wearable EEG device- Emotiv EPOC+	Dataset for Emotion Analysis Using Physiological Signals (DEAP) 3 construction site	Music, videos job sites stressors	OMTL-Covariance, OMTL-LogDet, OMTL-Vonneumann	OMTL-VonNeumann 71.14% - DEAP dataset 77.61% - construction site dataset	Near real-time stress recognition, reduce workers' injuries, accidents, and errors	/
[7]	ECG, EDA, respiration	Zephyr BioModule, Empatica E4, LG Watch Style	Laboratory settings-experimental room	socio-evaluative stressor and a cognitive stressor	Naïve Bayes, LibSVM, IBk, Multi-ClassClassifier, JRip, and Random Forest Neural network	three class - 78.7% two class – 98.3%	/	/
[8]	EEG	EEG reusable electrodes from supplier BIOKIT	Laboratory settings	Stroop color-word test	SVM	72.3%	/	/
[9]	ECG (Heart rate), PPG (Pulse rate), skin temperature and 3-axial acceleration	Toshiba Silmee Bar Type wearable sensor, Silmee W20/W212 wristband sensor	Office environment	/	k-Nearest Neighbour (k-NN), Decision Tree (DT) and Bagged Ensembles of Decision Trees (BE-DT)	Average accuracy of 70.60% for personalized approach and BE-DT	/	Larger study is required to confirm the significance of the results
[10]	EEG	Emotiv Epoc neuroheadset	Laboratory settings	Stroop colour-word test and mental arithmetic test	SVM	75%	/	/
[11]	ECG, EDA	Three-lead ECG sensor, two-lead EDA sensor attached on the BITalino - wearable sensor platform	Real life settings – relaxing periods and exam periods	Written exam and oral exam	SVM, Linear Discriminant Analysis, Ensemble, kNN, Decision Tree J4.8	91% with SVM	/	/
[12]	Face images, facial landmarks	General camera	Laboratory settings	Predefined experimental scenario	Deep neural network	64.63%	/	/
[13]	ECG, EDA, RSP (respiration), BVP (blood volume pulse), and SKT (skin temperature)	Shimmer3 ECG Unit and the Empatica E4 wristband	Laboratory settings	Four horror clips and a cognitive test	k-Nearest Neighbors (kNN) Decision Tree (DT) Random Forest (RF)	84.13%	/	/
[14]	HRV (extracted from ECG)	Three bipolar silver-chloride electrode pads	Laboratory settings	Trier social stress test	Fuzzy ARTMAP (FAM) neural network	Ensemble FAMs 80.57%	Processing salivary samples to derive the alpha-amylase and the cortisol as objective indicators of stress is a long and laborious process	/
[15]	Spatiotemporal behaviour of the head (i.e. head motion and head pose patterns)	High performance color camera – for video recording	Laboratory settings	Social Exposure, Emotional Recall, Stressful images/ Stroop Color Word Task, Stressful videos	K-nearest neighbours (K-nn), Generalized Likelihood Ratio (GLR), Support Vector Machines (SVM)	For social exposure K-nn =98.6 % GLR =97.9 % SVM =97.2 %	/	/
[16]	(ECG, PPG)-HRV	Wristband PPG device, Polar h10	Laboratory settings	Mental arithmetic	Random forest	5 min ECG-97.94%, 5 min PPG-98.48%	Consumer-grade wrist-based PPG sensor is used, which is affordable, convenient, and with reason- able accuracy as consumer ECG sensors	/

[17]	ECG-HRV	Two Ag/AgCl electrodes were placed in symmetric position of the chest	Laboratory settings	Social exposure, recall of a stressful event, cognitive load, watching of stressful videos	1-dimensional Deep Wide Convolutional Neural Network	89.9%	/	/
[18]	Handwriting and drawing	INTUOS WACOM series 4 digitizing tablet and a writing device- Intuos Inkpen	Laboratory settings	/	Random forest and SVM	Random Forest-60.2% SVM - 55 %	Providing a handwriting/ drawing database to the scientific community for further testing.	Involved a specific class of subjects (students) - does not allow for a generalization of the identified features
[19]	ECG signal (Heart Rate), Galvanic Skin Response and Respiration Rate	Pasco sensors	Laboratory settings - Multiplex 7D Cinema	Not specified	Artificial Neural Network – feedforward network	Accuracy-99% Sensitivity-98%	/	/
[20]	EEG	14-channel Emotiv device	Laboratory settings – flight scenario	Training program	LDA, 1-NN, SVM, Naïve Bayes	3 emotions with SVM 72.22% 4 workload levels with SVM 74.23%	/	/
[21]	Handwriting and signature	Pressure sensitive tablet called Wacom Intuos Pro – large (19"x12.5") and a writing device called Intuos Inkpen (Wacom Art Pen - KP701E2)	Laboratory settings	Video, time constrains for task performance	K-Nearest Neighbor (k-NN), JRIP and Random Forest	three class classification 55% - 58% for the handwriting 45% - 50% for the signature biometrics	Offline and online handwriting and signature biometric database with a wide range of ground truths (emotional status labels – happy, sad and stress) in addition to the identity labels	/
[22]	Body parts movements (Head, Shoulder, Elbow, Palm), Galvanic Skin Response (GSR) (fatigue, stress), Heart Rate (HR) (fatigue and stress), Skin Conductance Response (SCR) (fatigue)	Kinect sensor for movements of each subject, GSR and ECG sensors	Laboratory settings – indoor environment	Customized version of the Stroop Colour Word test	Fuzzy Inference Systems (FIS)	/	/	/
[23]	EDA	BioNeuro multichannel biofeedback instrument (Thought Technology, Canada)	Laboratory settings	Movie clips and images (International Affective Picture System (IAPS))	Particle swarm optimization (PSO)-k-nearest neighbor's algorithm (kNNs)	79.83±5.67%	/	/
[24]	ECG signal -heart rate, respiration, temperature and Skin Conductance	4 sensors with a NeXus-10 MKII, motion capture system VICON	Outdoor environment (controlled)	Disturbance command sent to the UAV	ANFIS (Adaptive neuro fuzzy inference system) model	/	/	/
[25]	Blood Volume Pulse, Galvanic Skin Response and Skin Temperature	eHealth sensor- left arms, palms and fingers	Laboratory settings	International Affective Picture System (IAPS)	decision tree (J48) and IBK classifiers	J48=98.63% IBK=97.4%	/	/
[26]	Combination of behavior data (body movement and hand movement) and weather conditions	Web-camera	Office settings	/	K-Nearest Neighbors (k-NN) Support Vector Machine (SVM) Decision Tree (D-Tree)	SVM algorithms generic model – 83% personalized model – 91%	/	/
[27]	EEG signal	MindWave Mobile sensor attached on forehead	Laboratory settings	Music	Deep back-propagation network	80.13%	/	/
[28]	Thermal data from five facial regions, electrodermal activity (EDA)	InfrREC R300SR-S high resolution infrared video camera, Empatica E3 electrodermal activity (EDA) sensor, modified version of MyKeepon robot	Laboratory settings	Two interactive sessions with a robot and three sets of video clips	Principal component analysis (PCA), logistic regression and a support vector machine (SVM)	77.5%	/	The sample size is small and results may not be representative of the larger population. The order of elicitation method might influence the classification results.
[29]	Human facial expressions associated with visual discomfort	Linear polarized stereoscopic display (Redrover SDM-400®), high definition camcorder (SONY HDR-XR350®)	Laboratory settings	Excessive screen disparities of stereoscopic three-dimensional (S3D) contents- 8 video sequences	binary SVM classifier with a RBF kernel	81.42%	Novel facial expression database regarding the visual discomfort	/
[30]	Interaction details (pressure, speed, duration, key type)	Android based custom keyboard	In-the-wild	/	LSTM (Long Short-Term Memory) encoder + multitask learning (MTL) based deep neural network (DNN)	84%	MTL is used to train the model using all users data vs relying only on personal data Automatic representation learning	/

A. Stress Recognition Based On Physiological Signals

a) *EEG (Electroencephalogram) signal* - is a neuro signal which is generated due to various electrical activities in the brain, and is measured using electrodes placed on the scalp. Several types of electrical activities correspond to different states of the brain, e.g., Alpha waves 7.5–13Hz, Beta waves 15–20Hz, Gamma waves 38–higher Hz, Delta waves 0.5–4Hz and Theta waves 4–7.5Hz. These signals can be captured and processed to get the useful information. The presence of stress can be identified by the changes of EEG Alpha and Beta power. Alpha activities are a sign of a calm and balanced state of mind and decrease in stressful states. Beta activity correlates with emotional and cognitive processes and increases with stress. A number of papers used EEG as for stress recognition.

The authors in [2] propose a procedure to automatically recognize workers' stress in construction sites using EEG

signals. EEG signals were obtained from 11 male workers working on three construction sites. Workers were exposed on two job site stressors: working hazards (working at the top of a ladder and working in a confined space) and tiredness (continuous work without taking a break time). Workers' salivary cortisol, that is frequently used as a biomarker of psychological stress, was also collected to label low or high-stress levels when working on construction sites. Different classification algorithms were employed: k-Nearest Neighbours (k-NN); Gaussian Discriminant Analysis (GDA); Support Vector Machine (SVM) with different similarity functions (linear, Gaussian, cubic, and quadratic). The results showed that the fixed windowing approach and the Gaussian Support Vector Machine, yielded the highest classification accuracy of 80.32% for two class classification, which is very promising, given the similar accuracy of stress recognition in clinical domains (where wired EEG devices were used and the subjects were engaged in minimal body movement).

EEG-based stress recognition framework that takes into account subject's brainwave patterns to train the stress recognition classifier and continuously update it, based on new input signals in near real-time is proposed in [6]. The proposed framework applies different Online Multi-Task Learning (OMTL) algorithms to recognize individuals' stress in near real time. The proposed framework was applied on the EEG collected in two environments. The first EEG dataset was collected in a controlled lab environment from 32 subjects using a wired-EEG (DEAP dataset). The second dataset was collected at in the field using a wearable EEG device, from 7 healthy workers on three real construction sites, while facing various stressors (working at the top of a ladder in a confined space). The OMTL-VonNeuman method resulted in the best prediction accuracy on both datasets (71.14% on the first and 77.61% on second dataset) among all tested algorithms (two class classification).

A system designed to classify three levels of stress: low, moderate and high stress, by means of EEG signal, is presented in [8]. A total of 132 signals from 12 subjects (aged 20 to 35 years) are collected. Validation of algorithm is carried out using Stroop Color Word Test (SCWT) as the stressor to induce various stress levels. Measure of stress is taken by means of questionnaires method. Discrete Wavelet Transform (DWT) is used for pre-processing and SVM is used as the classifier. Average accuracy for subject independent model is about 72.3%.

In [10] a framework for stress recognition based on power band features from EEG signals and relative difference of beta and alpha power as feature is proposed. A total of 10 subjects (9 male and 1 female.) participated in dataset acquisition experiment. All the subjects were healthy, at the age of 20 to 35 years. For stress elicitation SCWT and mental arithmetic test were utilized. With SVM as classifier, three-levels of stress can be recognized with an accuracy of 75%. For two-level stress analysis, accuracy of 88% and 96% are achieved for SCWT test and mental arithmetic test respectively.

EEG based human factors evaluation tools allows workload, emotion and stress recognition during the air traffic control operators' task performance with high temporal resolution [20]. Twelve air traffic control operators (ACTOs) participated in the two-hour training session on the novel air traffic control three-dimensional radar display. EEG is used to monitor the brain states of the ATCOs while they are learning to use the 2D+3D display. Training program was interrupted after 15, 60 and 120 minutes. SVM was used for three class emotion classification with achieved accuracy of 72.22% and for four class workload level classification with obtained accuracy of 74.23%.

In [27] a system which could collect multi-users' brainwaves, at the same time, is developed. The system's dataset consists of brainwaves from 7 test subjects. Each test subject has 10 minutes of brainwaves inducted by listening to the music. The system used this data to predict the test subjects mental state from their emitting brainwaves for each class, 1 (attention) and 0 (meditation). The achieved classification accuracy is 80.13%. The system classification method is a deep learning model with fully connected layers.

b) *ECG (Electrocardiogram)* - one of the most prominent signals for discriminating stress is the heart activity, as the Autonomous Nervous System (ANS) directly affects the heart rate. ECG is a standard heart rhythm measurement that track electrical impulses during the contraction and relaxation of the heart. For a standard threepoint ECG, three electrodes are placed on the subject's torso, measuring the depolarisation and repolarisation of the heart tissue during each heartbeat. Sampling rates of ECG devices range up to 1024 Hz. ECG is frequently used to extract information about Heart Rate (HR) and Heart Rate Variability (HRV).

The authors in [7] propose a stress state classification method by considering not only users' subjective evaluations but also temporal changes of stress responses in short periods. Dataset was obtained with measurement of ECG, Electrodermal activity (EDA) and respiration (RSP) signals from 40 subjects, 17 females and 23 males.

Dataset acquisition was performed in laboratory settings, where the stress induction was achieved by socio-evaluative stressor (interview in English) and a cognitive stressor (cross out alphabet "e"s in a document). Both the evaluation scores and the cortisol levels are utilized to classify labels of the collected data. Then, 6 machine learning algorithms (Naïve Bayes, LibSVM, IBk classifier, Multi-Class Classifier, JRip, and Random Forest Neural), as well as the implemented neural network algorithm based on the labeled data, were trained and tested for stress recognition. The achieved classification accuracy with neural network models are 78.7% for three class scenario and 98.3% for two class scenario. Binary stress recognition with the proposed classification method improves the recognition accuracy by up to 31.6% as compared to those with conventional techniques.

Features of the ECG and EDA signals were used as input for different classification methods (SVM, Linear Discriminant Analysis, Ensemble, kNN, Decision Tree J4.8) in [11]. Students, wearing sensors, were monitored in real life settings (during exams), in order to recognize the experienced stress levels. An experimental study was conducted with 10 students (4 male and 6 female, 19-26 years old), with no major health issues. The results revealed a recognition accuracy between 86-91% (the best classification results are achieved with SVM) for three classes, including relax state, written exam, and oral exam.

In [13] the physiological signals: ECG, EDA, RSP (respiration), BVP (blood volume pulse), and SKT (skin temperature) are acquired for stress recognition. Participants in the experiments included 30 subjects in the range of 25 to 35 years. Stress was elicited by four horror clips and a cognitive test (i.e., an arithmetic task - final stage of the Trier Social Stress Test) at the end. The horror clips have been selected from the Emotional Movie Database (EMDB). The experiments were conducted to induce two main states: no-stress and stress. Decision Tree (DT), k-Nearest Neighbors (kNN) and Random Forest (RF) were employed for dataset classification. The proposed multi-modal machine-learning algorithm, based on the random forest algorithm, was able to distinguish between the relaxing task and the intense cognitive task with an accuracy of 84.13%, on average. Moreover, the proposed multi-modal machine-learning algorithm also distinguishes between two different emotion states with an average accuracy of 83.33%.

ECG was used for stress recognition in articles [4] and [5] as well. In article [4] it was used together with EMG signal, and in article [5] it was combined with EDA, Electromyography (EMG) and Reaction Time (RT). These two articles will be analyzed in details in the following sections.

c) *Heart rate* - is the speed of the heartbeat measured by the number of contractions of the heart per unit of time, typically beats per minute (bpm). The heart rate can vary according to the body's physical needs, including the need to absorb oxygen and excrete carbon dioxide. It is usually equal or close to the pulse measured at any peripheral point. Activities that can provoke change include physical exercise, anxiety, stress, illness, ingesting drugs etc.

In [1] a test with 21 students was conducted and 21 physiological features of five signals (heart rate, skin temperature, galvanic skin response of the hand, oxygen saturation, and breath-flow rate) were analyzed. The stress induction protocol consisted of a neutral task, a non-stress task (listening to instrumental music), and a stress task (time-constrained arithmetic task). Four classifiers (SVM), k-NN, Random Forest and Logistic Regression) were compared to find the physiological feature subset that provides the best accuracy to identify states of stress and anxiety. Stress was identified with an accuracy greater than 90% (Kappa = 0.84) using the k-Nearest Neighbors classifier, using data from heart rate, skin temperature and oximetry signals and four physiological features. The identification of anxiety was achieved with an accuracy greater than 95% (Kappa = 0.90) using the SVM classifier with data from the galvanic skin response signal and three physiological features. Maximum achieved accuracy for two class stress recognition was 95.98% obtained with k-NN (5 signals, 13 features), while for anxiety recognition 98.89% was obtained with SVM (3 signals, 6 features).

Heart rate, respiration rate, foot galvanic skin response and hand galvanic skin response were used for stress recognition task in [19]. Artificial Neural Network (ANN) was trained using data from Physionet database as well as data collected from other researchers. Developed neural network was validated with 77 samples. Samples were obtained from subjects in 7D cinemas. Output data was classified into two output classes: stress and no stress. The achieved accuracy with the proposed method was 99% and sensitivity was 98%.

The article [24] presents a prototype that monitors the physiological conditions of the pilot in order to recognize the altered states that have occurred. If the system recognizes the certain stress condition, the system overrides the pilot's commands, which under altered (stress) states may be erroneous. Thus, the system takes over the command of the plane UAV (Unmanned Aerial Vehicle) in order to perform a safe routine flight such as landing or flying back to a safe location. This test was performed with 13 subjects, once per person. ECG signal-heart rate, respiration, temperature and skin conductance were collected in dataset acquisition phase. The experiments were conducted outdoor, introducing stress with disturbance command sent to the UAV. For the test with the ANFIS (Adaptive Neuro Fuzzy InferenceSystem) model, 3 different types of models (Grid Partitioning, Subtractive Grouping, and fuzzy c-means) were used, from which the fuzzy c-means showed best results in the prediction of values.

In [9] heart rate, PPG (Pulse rate), skin temperature and 3-axial acceleration were used for automatic stress recognition. In this paper the dataset was acquired in office environment from 4 users without stress induction methods. The participants were observed 11 working days, resulting in 44 segments per user. In total, 352 hours of physiological data was collected. An advanced multi-classification model of 8 distinct moods and 5 levels of intensity, operating on 2-hour time windows is proposed. k-NN, Decision Tree (DT) and Bagged Ensembles of Decision Trees (BE-DT) algorithms were employed for data classification. The most predictable mood, in terms of classification accuracy of the personalized model, is Anger followed by Sadness, Happiness, Stress, Tiredness, Boredom and the least is Calmness. Average accuracy of 70.60% for personalized approach and BE-DT was achieved.

Heart rate was used for stress recognition in [22] as well. Here it was combined with behavioural signals: Galvanic Skin Response (GSR), and Skin Conductance Response (SCR). This paper will be analyzed in details in the following section.

d) *Heart Rate Variability (HRV)* - is also a common measure of human stress state, as it reveals the balance between the sympathetic and parasympathetic nervous system. When the sympathetic nervous system is triggered, and the parasympathetic system is suppressed, which is called fight-or-flight reaction, epinephrine and nor-epinephrine hormones are secreted. This process evokes the increase of blood pressure (BP), heart rate (HR), muscle tension, skin conductance, and the decrease of HRV. When parasympathetic system is activated and sympathetic system is suppressed, which is called relax and digest process, the opposite physiological response as that of fight-or-flight process will be triggered. Generally, HRV features are generated from the successive R-R intervals of ECG.

Authors in [14] measured the salivary alpha-amylase and cortisol as objective measures of stress. These data were then correlated with the HRV features using fuzzy ARTMAP (FAM) neural network. A total of 176 ECG recordings and 264 salivary samples were obtained from 22 subjects while performing Trier Social Stress Test. 17 male and 5 females subjects, with an average age of 21 years, participated in this research. The ensemble of FAMs is used for predicting stress

responses of salivary alpha-amylase or cortisol using heart rate measurements as the input. Using alpha-amylase as the stress indicator, the ensemble was able to classify stress from heart rate features with 75% accuracy, and 80% accuracy when cortisol was used.

HRV extracted from PPG and ECG signals is used for stress recognition in [16]. The experiment was performed with six healthy participants (ages 21-40 years), performing mental arithmetic. The result shows that ten HRV parameters have significant differences between stress and non-stress states. Furthermore, the 10-fold accuracy of stress state detection within subjects is 98% and the Leave-One-Participant-Out F1 score reaches 80% with Random Forest algorithm. The results demonstrate that wrist-based PPG can provide HRV measurements that enable the recognition of mental stress as accurately as ECG, even for a short three-minute temporal window.

Authors in [17] proposes a 1-dimensional Deep Wide Convolutional Neural Network with 6-fold cross-validation for stress recognition, based on HRV signal. The proposed methodology outperforms single kernel networks achieving classification accuracy up to 99.1%, better overall performance (avg. F1score 88.1%, avg. accuracy 89.8%) and more consistent behaviour across study's experimental phases. 24 participants (7 women and 17 men) participated in this study. In order to investigate the effects of stress conditions, stress experiment that included social exposure, recall of a stressful event, cognitive load, and watching of stressful videos, was designed and developed,

e) *Blood Volume Pulse (BVP)* - is the measure of the volume of blood that passes over a PPG sensor with each pulse. Photoplethysmography (PPG) is the low-cost optical technique to measure BVP. It uses the absorption of light by blood. After light is emitted from a light source, different amounts of blood in the volume will absorb different amount of light. In this manner, blood volume can be measured.

In [25] a system for recognizing several emotional states like 'Sad', 'Dislike', 'Joy', 'Stress', 'Normal', 'No-Idea', 'Positive' and 'Negative' based on BVP, GSR and Skin Temperature is proposed. Dataset is obtained from 24 participants; each experiment took from 11 to 12 minutes; the sample rate of all physiological sensors were 650 Hz. Emotion elicitation was performed with International Affective Picture System (IAPS). Decision tree (J48) and IBk classifiers were utilized for dataset classification. The results indicate that the system has an accuracy rate of approximately 97% with IBk and 98% with J48.

BVP together with ECG, EDA, respiration and skin temperature, was already used to identify stress in the article [13].

f) *The Electrodermal Activity (EDA)* - is defined as a change in the electrical properties of a person's skin, caused by an interaction between environmental events and the individual's psychological state. EDA is commonly measured at locations with a high density of sweat glands, e.g. palm/finger or feet, by means of two electrodes placed on the skin surface, next to each other, while applying a weak electrical current between them. The minimal sampling rate to decompose the EDA signal into skin conductance level and skin conductance response contributions is around 30 Hz.

In [5] EDA, ECG and Electromyography (EMG) as well as Reaction Time (RT) are recorded for the purpose of stress recognition. 22 students, divided in two groups, participated in the study. The first group of 10 male students participated into the experiment of visual stressor (Stroop test) while the second group of 12 female students participated in the experiment of auditory stressor. Using physiological signals as well as RT, a classifier based on the SVM was developed. The strategy of recognition using the decision fusion is presented in this paper. The recognition is achieved by fusing the classification results of physiological signals and RT with the voting method. For two class classification problem visual stressor gave over 83.3% accuracy (up to 100% for different subjects), and auditory stressor gave over 71.4% (up to 100% for different subjects).

In [23] the authors utilized movie clips and images from International Affective Picture System (IAPS) to evoke emotion in athletes. The experimental paradigm designed for emotion induction effectively aroused four common emotions: calmness, sadness, fear, and happiness. Ten subjects, 6 males and 4 females, participated in the experiments. The indoor temperature was controlled at around 20°C. In this way, 86 samples of EDA data were determined for the four emotions. To improve recognition accuracy, the captured emotions were subjected to baseline removal and Particle Swarm Optimization (PSO) feature. The emotional model for the athletes was set up based on the emotional probability space of the Markov Chain. The proposed method achieved recognition accuracy of 79.83±5.67% with PSO – kNNs algorithm.

Stress recognition based on EDA was also employed in other papers that were subject of analysis [1, 7, 11, 19, 24, 25].

g) *Electromyogram (EMG)* - measures muscle action potentials by placing electrodes on selected muscles. Facial and Trapezius muscles are regions of interests for measuring muscle activity. The mean, median, standard deviation, RMS, peak loads and gaps per minute are the features that are used commonly.

In [4] both EMG and ECG signals were acquired simultaneously from 34 healthy students (23 females and 11 males, aged 20-37 years). Mental arithmetic, SCWT, under time pressure, and stressful environment were employed to induce stress in the laboratory. Well-trained SVM classifier was employed as a detection model to map the stress to two, three and four different levels. The accuracies of stress recognition in two, three and four levels were 100%, 97.6%, and 96.2%, respectively. These were obtained from the distinct combination of feature selection and machine learning algorithms-SVM with RBF kernel. It was found that EMG signal of the right trapezius muscle recognizes stress better than other muscles.

EMG signal combined with EDA, ECG and Reaction Time was also utilized for stress detection in article [5] (presented in previous section).

h) *Skin temperature* - the average body temperature of an individual is around 36°C-37°C. Stress effects result in changes in body temperature. Acute stress triggers peripheral vasoconstriction, causing a rapid, short-term drop in skin temperature in homeotherms.

Skin temperature in combination with other physiological signals has been used in many studies [1, 12, 21, 23]. All these articles have already been analyzed in the previous sections.

i) *Respiration (RR)* - also known as ventilation rate or ventilation frequency, is the number of breaths (inhalation-exhalation cycles) taken within a set amount of time (typically 60 seconds). Human respiration rate is measured when a person is at rest and involves counting the number of breaths for one minute by counting how many times the chest rises. Commonly a chest belt (Respiratory Inductive Plethysmograph - RIP), which is either worn thoracically or abdominally, is utilized to measure the respiration pattern directly.

Respiration rate or breath-flow rate or breathing rate is combined with other physiological signals in articles [1], [7], [13], [19] and [24] to build stress recognition systems. All these papers are already presented in the above sections.

j) *Thermal Images* – because stressed persons suffer from temperature changes, stress states can also be recognized from thermal images, taken with infrared camera. This signal acquisition method is unobtrusive and thus interesting for development of stress recognition systems.

In [3], authors are focused on the establishment of a set of non-contact imaging-based classifications for Emotional Stress (ES) and Physical Stress (PS). A total of 60 healthy volunteers with different skin colours (Caucasians, Indians, Chinese, Malaysians, and South Africans) and different genders (55% male and 45% female) participated in the experimental trials. Stress was induced with heavy running, and Trier Social Stress Test (public speaking in the form of an interview, mental arithmetic, and recognition memory task). Classification algorithm based on signal amplification and correlation analysis called Eulerian magnification-canonical correlation analysis is proposed. This signal amplification algorithm expands the signals of ES and PS in different frequency domains. Sparse coding and canonical correlation analysis then fuse the original signal and its amplified features. The extracted entropy features are used to train the correlation weight between ES and PS, which formulates stress classifications. With the new classification method, based on Back Propagation (BP) neural network, it was achieved an accuracy rate of 90%.

In [28], the efficacy of using a far infrared (FIR) camera for detecting robot-elicited affective response compared to video-elicited affective response by tracking thermal changes in five areas of the face, is evaluated. Ten healthy adults participated in the study for a duration of approximately 30 minutes. Localized changes in the face are analyzed in order to assess whether the thermal or electrodermal responses to emotions, evoked by traditional video techniques and by robots, are similar. Finally, principal component analysis is performed to reduce the dimensionality of data and to evaluate the performance using machine learning techniques (SVM 2-state emotion classifier) for classifying thermal data by emotion state, resulting in a thermal classifier with a performance accuracy of 77.5%.

B. Stress Recognition Based On Behavioral Signals

a) *Body gestures and movements* - body language refers to the nonverbal signals that we use to communicate. According to experts, these nonverbal signals make up a huge part of daily communication. From our facial expressions to our body movements, the things we don't say can still convey volumes of information. Persons under stress show various changes in behavior as well as changes in body movement or body gestures, like: jaw clenching, arm movements, self-touching, finger rubbing, posture change etc.

Features related to head movements and pose were computationally estimated and analyzed in [15]. Towards this direction, facial landmarks were fitted using Active Appearance Models (AAM). The population of this study were 24 participants (7 women, 17 men) with age 47.3±9.3 years. The participants were exposed on Social Exposure, Emotional Recall, Stressful images/ SCWT, and Stressful videos. Data recordings belong to Semeoticons Reference Dataset for Stress Assessment SRDSA'15. Results indicate that specific stress conditions increase head mobility and mobility velocity, in both translational and rotational features. For dataset classification k-NN, Generalized Likelihood Ratio (GLR), and SVM were utilized. The highest classification accuracy (for 2 class scenario) was obtained during social exposure which includes the interview task: k-NN =98.6 %, GLR =97.9 %, and SVM =97.2 %.

In [22] authors propose a framework for recognition of stress and fatigue based on affective and corporal indicators: body parts movements (head, shoulder, elbow, palm), GSR, HR and SCR. The framework has been experimentally validated on a dataset of 25 subjects. The dataset consists of 1064 intervals of 20 sec. each for both GSR and HR recordings. Stress was evoked with customized version of the SCWT. The average of GSR and HR, as well as the frequency of SCR occurrences were calculated for each interval. The inference system takes the values of the GSR and HR features, as input, and based on a set of appropriate fuzzy rules (Fuzzy Inference Systems-FIS), calculates an estimation regarding the subject's stress level, encoded in the range [0, 1]. At the authentication stage, each movement is compared to the corresponding template signatures via the HMM classification algorithm, and the returned probability is held as the matching score. It should be mentioned that the proposed framework decreases the FAR (False Acceptance Rate) and FRR (False Rejection Rate) in the equal error rate-EER point from 7.8% to less than 3.2%.

Well-being recognition system where a deep learning technique is adopted to provide a non-invasive monitoring system in an office setting is proposed in [26]. The experiment was conducted on two human subjects in office environment without stress induction. The monitoring process lasted for a total of 60 days. The system extracted behaviour data (body movement and hand movement) using the trained body and hand detector based on a Faster Region-based Convolutional Neural Network (Faster R-CNN). The classification of the well-being level was performed with three features from two surveys, which covered both stress and mood. The employed classifiers were k-NN, SVM with linear kernel function and Gaussian kernel function, and Decision Tree (D-Tree). The achieved accuracy with SVM (binary classification problem) was 83% on generic model and 91% on a personalized model.

b) *Facial expressions* - stress and emotional states have a correlation with facial expressions, and thus can be recognized from them.

In [12] a method for recognizing stress by extracting high-dimensional features from face images acquired by a general

camera is proposed. Fifty subjects took part in the experiment, with predefined scenario. The total number of collected images was 242,730 divided in three classes – no stress, weak stress and strong stress. In the proposed deep neural network, the face images and face landmarks detected earlier, are inputted to output stress recognition results. The achieved classification accuracy is 64.63%. Shortcut mapping and bottleneck architecture are used to optimize neural network structure. It is found that facial landmarks are better at perceiving stress because they allow us to better understand eye, mouth, and head movements.

The authors of the paper [29] investigate human facial expressions associated with visual discomfort, from a face captured by a camera. The visual discomfort was induced by excessive screen disparities of stereoscopic three-dimensional (S3D) contents - 8 video sequences (10 second length and about 300 frames per video). The acquired database contained approximately 230 face videos (696,000 frames) from 29 adult participants (21 males and 8 females). The relevance scores (confidence values) between the facial expressions caused by the visual discomfort and the six emotional facial expressions ("stressed", "fear", "happiness", "sadness", "surprise" and "neutral") were measured. As a result, it is observed that the emotional facial expression of "stressed" (i.e., anger or disgust) highly correlated with visual discomfort (Pearson correlation coefficient: 0.91). Based on this observation, a simple and practical discomfort measurement method (+1 for the class "Discomfort" and -1 for the class "Comfort") was designed and its feasibility was successfully verified (classification accuracy of 81.42% achieved with binary SVM classifier with a RBF kernel).

c) *Handwriting and drawing* - provides opportunities for personal characteristics estimation, particularly, emotional state. These biometrics can be represented in two ways: off-line and on-line. The input of the off-line systems is an image of a written text; the image is pre-processed by grey scaling, removing noise and segmenting characters and words. On the other hand, on-line systems take the input through an electronic pen used during the handwriting/ drawing/ signature process.

In paper [18] the first publicly available database which relates emotional states to handwriting and drawing, so called EMOTHAW (EMOTion recognition from HAndWriting and draWing) is presented. This database includes samples of 129 participants whose emotional states, namely anxiety, depression and stress, are assessed by the Depression–Anxiety–Stress Scales (DASS) questionnaire. During data acquisition process the subjects were performing seven different writing or drawing tasks: drawing predefined objects/lines, writing in printed/cursive letters. Records consist in pen positions, on-paper and in-air, time stamp, pressure, pen azimuth, and altitude. Although the depression recognition systems have the best overall accuracies, they are the worst in ROC (Receiver operating characteristic) space. Stress recognition with Random forest based on drawing and writing features achieved 60.2% accuracy, while stress recognition with SVM obtained 55% accuracy.

In [21] a system for stress recognition based on handwriting and signature biometrics is proposed. The database comprised of a total of 134 participants with 804 handwriting and 8040 signature biometric samples. The participants performed 2 text-dependent and 2 text-independent tasks. Video and time constrain were applied during task performance. This study focuses on the online features collecting path and time dependent features, since on-line systems generally perform better than their off-line counterparts. k-NN, JRIP and Random Forest were utilized as classification algorithms in three class scenario (happy, sad and stress). Considering handwriting and signature biometrics, the best prediction accuracy is achieved using a Random Forest classifier with accuracy between 55% - 58% for the handwriting and 45% - 50% for the signature biometrics.

d) *Keystroke dynamics* – various subjects have different keyboard writing speed and style. The muscles of the stressed individual contract much more than regular, which affects the pressing of the keyboard. Thus the Keystroke dynamic can be use as a valid behaviour data for stress detection.

In [30] stress recognition method that utilizes keystroke interaction details (pressure, speed, duration and key type) is presented. The classification dataset was acquired during 3-week in-the-wild study involving 24 participants (20 male and 4 female). A custom keyboard capable of tracing users' interaction pattern during text entry was used. Interaction details like touch speed, error rate, pressure and self-reported emotions (happy, sad, stressed, and relaxed) were collected during the study. The analysis on the collected dataset reveals that the representation learned from the interaction pattern has an average correlation of 0.901 within the same emotion and 0.811 between different emotions. As a result, the representation is effective in distinguishing different emotions with an average accuracy (AUCROC) of 84% with LSTM (Long Short-Term Memory) encoder combined with multitask learning (MTL) based deep neural network (DNN).

IV. DISCUSSION AND CONCLUSION

The aim of this review was to provide an overview of stress recognition systems, along with the techniques and methods used. Although different modalities can be used to recognize stress, the most dominant method for recognizing stress is physiological signals. From 30 analyzed articles in this review study, systems for stress recognition based on physiological signals are proposed in 22 articles; the other 8 papers use behavioral signals. From the physiological signals only EEG was used independently, the other signals were used in combination with other signals. Most widely used signal is ECG and its derivatives: heart rate and heart rate variability;

For classification of the acquired datasets the following machine learning algorithms were used: k-Nearest Neighbours, SVM –Support Vector Machine, Random Forest, JRIP, GDA - Gaussian Discriminant Analysis, IBk classifier, LR – Logistic Regression. In a number of stress/emotion recognition methods neuro fuzzy logic is presented: deep learning model, ANFIS (adaptive network-based fuzzy inference system), fuzzy ARTMAP (FAM), deep wide Convolutional Neural Network (CNN), LSTM (Long Short-Term Memory) encoder combined with multitask learning (MTL) based deep neural network (DNN).

The proposed stress recognition techniques are tested on different datasets. Different number of participants took place in the different experiments. The duration of time series as well as the number of collected images varies depending on the scenario. Further, the classification problems are not

unified: the number of classes varies from 2 to 8. Thus, it is very difficult to conclude which machine learning technique or neuro fuzzy system is most suitable for stress detection. For three class scenarios, classification accuracy goes over 70%, for two class scenario the obtained classification accuracy can be over 95%, in some articles even 99%. The authors report SVM as most successful machine learning technique for stress recognition.

For further research in the corresponding field it will be challenging to employ, more intensively, some up to date neural network architectures, like deep convolutional neural networks. Additional boosting of classification accuracy in those systems can be obtained by usage of ensembles of CNN with voting method.

REFERENCES

[1] Rodríguez-Arce, J., Lara-Flores, L., Portillo-Rodríguez, O., & Martínez-Méndez, R. (2020). Towards an anxiety and stress recognition system for academic environments based on physiological features. Computer methods and programs in biomedicine, 190, 105408.

[2] Jebelli, H., Hwang, S., & Lee, S. (2018). EEG-based workers' stress recognition at construction sites. Automation in Construction, 93, 315-324.

[3] Hong, K., Liu, G., Chen, W., & Hong, S. (2018). Classification of the emotional stress and physical stress using signal magnification and canonical correlation analysis. Pattern Recognition, 77, 140-149.

[4] Pourmohammadi, S., & Maleki, A. (2020). Stress detection using ECG and EMG signals: A comprehensive study. Computer methods and programs in biomedicine, 193, 105482.

[5] Zhang, B., Morère, Y., Sieler, L., Langlet, C., Bolmont, B., & Bourhis, G. (2017). Reaction time and physiological signals for stress recognition. Biomedical Signal Processing and Control, 38, 100-107.

[6] Jebelli, H., Khalili, M. M., & Lee, S. (2018). A continuously updated, computationally efficient stress recognition framework using electroencephalogram (EEG) by applying online multitask learning algorithms (OMTL). IEEE journal of biomedical and health informatics, 23(5), 1928-1939.

[7] Moon, J., Lee, J., Cheon, D., Lee, M., & Lee, K. (2019, November). Stress Recognition with State Classification Considering Temporal Variation of Stress Responses. In 2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM) (pp. 2852-2859). IEEE.

[8] Gaikwad, P., & Paithane, A. N. (2017, July). Novel approach for stress recognition using EEG signal by SVM classifier. In 2017 International Conference on Computing Methodologies and Communication (ICCMC) (pp. 967-971). IEEE.

[9] Zenonos, A., Khan, A., Kalogridis, G., Vatsikas, S., Lewis, T., & Sooriyabandara, M. (2016, March). HealthyOffice: Mood recognition at work using smartphones and wearable sensors. In 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops) (pp. 1-6). IEEE.

[10] Jun, G., & Smitha, K. G. (2016, October). EEG based stress level identification. In 2016 IEEE international conference on systems, man, and cybernetics (SMC) (pp. 003270-003274). IEEE.

[11] Hasanbasic, A., Spahic, M., Bosnjic, D., Mesic, V., & Jahic, O. (2019, March). Recognition of stress levels among students with wearable sensors. In 2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH) (pp. 1-4). IEEE.

[12] Jeon, T., Bae, H., Lee, Y., Jang, S., & Lee, S. (2020, January). Stress Recognition using Face Images and Facial Landmarks. In 2020 International Conference on Electronics, Information, and Communication (ICEIC) (pp. 1-3). IEEE.

[13] Montesinos, V., Dell'Agnola, F., Arza, A., Aminifar, A., & Atienza, D. (2019, July). Multi-modal acute stress recognition using off-the-shelf wearable devices. In 2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC) (pp. 2196-2201). IEEE.

[14] Liew, W. S., Seera, M., Loo, C. K., Lim, E., & Kubota, N. (2015). Classifying stress from heart rate variability using salivary biomarkers as reference. IEEE transactions on neural networks and learning systems, 27(10), 2035-2046.

[15] Giannakakis, G., Manousos, D., Chaniotakis, V., & Tsiknakis, M. (2018, March). Evaluation of head pose features for stress detection and classification. In 2018 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI) (pp. 406-409). IEEE.

[16] Chen, C., Li, C., Tsai, C. W., & Deng, X. (2019, May). Evaluation of mental stress and heart rate variability derived from wrist-based photoplethysmography. In 2019 IEEE Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS) (pp. 65-68). IEEE.

[17] Giannakakis, G., Trivizakis, E., Tsiknakis, M., & Marias, K. (2019, September). A novel multi-kernel 1D convolutional neural network for stress recognition from ECG. In 2019 8th International Conference on Affective Computing and Intelligent Interaction Workshops and Demos (ACIIW) (pp. 1-4). IEEE.

[18] Likforman-Sulem, L., Esposito, A., Faundez-Zanuy, M., Clémençon, S., & Cordasco, G. (2017). EMOTHAW: A novel database for emotional state recognition from handwriting and drawing. IEEE Transactions on Human-Machine Systems, 47(2), 273-284.

[19] Alić, B., Sejdinović, D., Gurbeta, L., & Badnjevic, A. (2016, June). Classification of stress recognition using artificial neural network. In 2016 5th Mediterranean Conference on Embedded Computing (MECO) (pp. 297-300). IEEE.

[20] Liu, Y., Lan, Z., Traspsilawati, F., Sourina, O., Chen, C. H., & Müller-Wittig, W. (2019, October). EEG-based Human Factors Evaluation of Air Traffic Control Operators (ATCOs) for Optimal Training. In 2019 International Conference on Cyberworlds (CW) (pp. 253-260). IEEE.

[21] Ayzeren, Y. B., Erbilek, M., & Çelebi, E. (2019). Emotional state prediction from online handwriting and signature biometrics. IEEE Access, 7, 164759-164774.

[22] Drosou, A., Giakoumis, D., & Tzovaras, D. (2017, June). Affective state aware biometric recognition. In 2017 International conference on engineering, technology and innovation (ICE/ITMC) (pp. 601-610). IEEE..

[23] Liu, Y., & Jiang, C. (2019). Recognition of shooter's emotions under stress based on affective computing. IEEE Access, 7, 62338-62343.

[24] Corichi, E. Z., Carranza, J. M., Garca, C. A. R., & Pineda, L. V. (2017, October). Real-time prediction of altered states in Drone pilots using physiological signals. In 2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS) (pp. 246-251). IEEE.

[25] Khan, A. M., & Lawo, M. (2016, September). Developing a system for recognizing the emotional states using physiological devices. In 2016 12th International Conference on Intelligent Environments (IE) (pp. 48-53). IEEE.

[26] Lawanot, W., Inoue, M., Yokemura, T., Mongkolnam, P., & Nukoolkit, C. (2019, January). Daily stress and mood recognition system using deep learning and fuzzy clustering for promoting better well-being. In 2019 IEEE International Conference on Consumer Electronics (ICCE) (pp. 1-6). IEEE.

[27] Liao, C. Y., Chen, R. C., & Tai, S. K. (2018, April). Emotion stress detection using EEG signal and deep learning technologies. In 2018 IEEE International Conference on Applied System Invention (ICASI) (pp. 90-93). IEEE.

[28] Boccanfuso, L., Wang, Q., Leite, I., Li, B., Torres, C., Chen, L., ... & Shic, F. (2016, August). A thermal emotion classifier for improved human-robot interaction. In 2016 25th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN) (pp. 718-723). IEEE.

[29] Lee, S. I., Lee, S. H., Plataniotis, K. N., & Ro, Y. M. (2016). Experimental investigation of facial expressions associated with visual discomfort: feasibility study toward an objective measurement of visual discomfort based on facial expression. Journal of Display Technology, 12(12), 1785-1797..

[30] Ghosh, S., Goenka, S., Ganguly, N., Mitra, B., & De, P. (2019, September). Representation Learning for Emotion Recognition from Smartphone Keyboard Interactions. In 2019 8th International Conference on Affective Computing and Intelligent Interaction (ACII) (pp. 704-710). IEEE.