ICONCS

2023

INTERNATIONAL CONFERENCE ON
CYBER SECURITY AND COMPUTER SCIENCE

PROCEEDING BOOK
2023

2023

PROCEEDING BOOK

ICONCS 2023

International Conference on Cyber Security and Computer Science

6-7 May 2023 / Safranbolu, Turkey

Organized by

Karabuk University

Proceeding Book of the International Conference on Cyber Security and Computer Science (ICONCS 2023)

Editors

Prof. Dr. Touhid BHUIYAN

Assoc.Prof.Dr. Muhammet Tahir GÜNESER

Asst.Prof.Dr. Caner ÖZCAN

Asst.Prof.Dr. Cihat ŞEKER

Asst.Prof.Dr. Emrah ÖZKAYNAK

Lect. Fatih GÜLTEKİN

Res. Asst. Betül KARAOĞLAN

Res.Asst. İbrahim Ethem YILMAZ

Res.Asst. İdris KAHRAMAN

https://iconcs.karabuk.edu.tr/

iconcs@karabuk.edu.tr

SCIENTIFIC COMMITTEE

Prof.Dr. Aslıhan TÜFEKÇI, Gazi University, Türkiye

Prof.Dr. Ertuğrul KARAÇUHA, Istanbul Technical University, Türkiye

Prof.Dr. Hasari ÇELEBİ, Gebze Technical University, Turkey (Senior Member, IEEE)

Prof.Dr. Huseyin SEKER, Northumbria University, UK

Prof.Dr. İbrahim SOĞUKPINAR, Gebze Technical University, Türkiye

Prof.Dr. İsmail R. KARAŞ, Karabük University, Türkiye

Prof.Dr. Mihai CERNAT, Stefan cel Mare University of Suceava, Romania (Fellow, IEEE)

Prof.Dr. Mustafa Servet KIRAN, Konya Technical University, Türkiye

Prof.Dr. Oguz FINDIK, Karabük University, Türkiye

Prof.Dr. Okan ERSOY, Purdue University, USA, (Fellow, IEEE)

Prof.Dr. Touhid BHUIYAN, Daffodil International University (Member, IEEE)

Prof.Dr. Sheak Rashed Haider Noori, Daffodil International University

Prof.Dr. Md. Ismail Jabiullah, Daffodil International University

Prof.Dr. Md. Fokhray Hossain, Daffodil International University

Prof.Dr. Monzur Morshed, Daffodil International University

Prof.Dr. Mohammad Shamsul Arefin, Daffodil International University

Assoc.Prof.Dr. Abdulkadir KARACI, Samsun University, Türkiye

Assoc.Prof.Dr. Mehmet GÖKTÜRK, Gebze Technical University, Türkiye

Assoc.Prof.Dr. Adib HABBAL, Karabük University, Türkiye

Assoc.Prof.Dr. Burhan SELÇUK, Karabük University, Türkiye

Assoc.Prof.Dr. Enver ÖZDEMİR, Istanbul Technical University

Assoc.Prof.Dr. Hakan KUTUCU, Karabük University, Türkiye

Assoc.Prof.Dr. Ilhami Muharrem ORAK, Karabük University, Türkiye

Assoc.Prof.Dr. Ilker TÜRKER, Karabük University, Türkiye

Assoc.Prof.Dr. M. Ali AYDIN, Istanbul University, Türkiye

Assoc.Prof.Dr. Mehmet HACIBEYOGLU, N.Erbakan University

Assoc.Prof.Dr. M. Tahir GÜNEŞER, Karabük University

Assoc.Prof.Dr. Nursel YALÇIN, Gazi University, Türkiye

Assoc.Prof.Dr. Ong Bi Lynn, UniMAP, Malaysia

Asst.Prof.Dr. Erkan ÇETINER, Bulent Ecevit University

Dr. Muhammad Nazrul Islam, Military Institute of Science and Technology, Bangladesh

Dr. Kazi Tanvir Ahmmed, University of Chittagong, Bangladesh

Asst.Prof.Dr. Ferhat ATASOY, Karabük University, Türkiye

Ts.Dr. Nik Adilah Hanin Zahri, UniMAP, Malaysia

Asst.Prof.Dr. Hakan YILMAZ, Karabük University, Türkiye

Dr. Naimah Yaakob, UniMAP, Malaysia

Ts.Dr. Ku Nurul Fazira Ku Azir, UniMAP, Malaysia

Dr. Shahrul Nizam Yaakob, UniMAP, Malaysia

Ts.Dr. Phaklen Ehkan, UniMAP, Malaysia

Asst.Prof.Dr. Emrah ÖZKAYNAK, Karabük University

Dr. Rozmie Razif Othman, UniMAP, Malaysia

Asst.Prof.Dr. İsa AVCI, Karabük University, Türkiye

Dr. Latifah Munirah Kamarudin, UniMAP, Malaysia

Asst.Prof.Dr. Nesrin AYDIN ATASOY, Karabük University, Türkiye

Asst.Prof.Dr. Moushumi Zaman Bonny, Daffodil International University

Dr. Ruzelita Ngadiran, UniMAP, Malaysia

Asst.Prof.Dr. Kasım ÖZACAR, Karabük University, Türkiye

Asst.Prof.Dr. Tarik Adnan ALMOHAMAD, Karabük University

Dr. Muhammad Imran Ahmad, UniMAP, Malaysia

Asst.Prof.Dr. Onur INAN, Selçuk University, Türkiye

Dr. Norsuhaida Ahmad, UniMAP, Malaysia

Asst.Prof.Dr. Safak BAYIR, Karabük University, Türkiye

Dr. Zahereel Ishwar Abdul Khalib, UniMAP, Malaysia

Dr. Rafikha Aliana A. Raof, UniMAP, Malaysia

Dr. Amiza Amir, UniMAP, Malaysia

Dr. Yasmin Mohd Yacob, UniMAP, Malaysia

Dr. Abdrakhmanov RUSTAM, Ahmet Yesevi University, Türkiye

Dr. Amirtayev KANAT, Ahmet Yesevi University, Türkiye

Bayezid Islam, Rajshahi University of Engineering & Technology (RUET), Bangladesh

Sourav Roy, KUET, Bangladesh

Al-Farabi Akash, Ahsanullah University of Science and Technology, Bangladesh

Shah Md. Salimullah, Bangladesh Army International University of Science and Technology, Bangladesh

Md. Saiful Islam, SAir AIR BD Ltd, Bangladesh

Liton Chandra Paul, Pabna University of Science and Technology, Bangladesh

Subrato Bharati, Ranada Prasad Shaha University, Bangladesh

Nayan Banik, Green University of Bangladesh, Bangladesh

Mosabber Uddin Ahmed, University of Dhaka, Bangladesh

Md. Sakibul Islam, Shahajalal University of Science and Technology, Bangladesh

Sampad Ghosh, Kyushu University, Japan

Mohammad Ali Moni, University of Sydney, Australia

Md Gulzar Hussain, Green University of Bangladesh

PRAJOY PODDER, BUET, Bangladesh

Shadman Sakib, University of Hyogo, Japan

Mahmudul Hasan, Ministry of Science and Technology, Bangladesh

Piyas Saha, Bangladesh Army University of Engineering and Technology, Bangladesh

Muhammad Kamal Hossen, Chittagong University of Engineering & Technology, Bangladesh

Md. Anik Hossain, City University, Bangladesh

Tamim Al Mahmud, Green University of Bangladesh

Manahan Siallagan, Institute Teknologi Bandung, Indonesia

ORGANIZING COMMITTEE

Honorary Committee

Prof.Dr. Refik POLAT, Karabük University, Chancellor

Prof.Dr. Ismail Koyuncu, Istanbul Tecnical University, Chancellor

Prof.Dr. Hacı Ali MANTAR, Gebze Tecnical University, Chancellor

Dr.Md. Sabur Khan, Daffodil International University, Chairman

Chair

Assoc.Prof.Dr. Muhammet Tahir GÜNESER, Karabük University, Türkiye

Co-Chair

Asst.Prof.Dr. Caner ÖZCAN, Karabük University

Asst.Prof.Dr. Cihat ŞEKER, Karabük University

Asst.Prof.Dr. Emrah ÖZKAYNAK, Karabük University

Technical Committee

Lect. Fatih GÜLTEKİN, Karabük University

Res.Asst. Betül KARAOĞLAN, Karabük University

Res.Asst. İbrahim Ethem YILMAZ, Karabük University

Res.Asst. İdris KAHRAMAN, Karabük University

Organization Committee

Prof.Dr. Ertuğrul KARAÇUHA, Istanbul Technical University

Prof.Dr. İbrahim SOĞUKPINAR, Gebze Technical University

Prof.Dr. Oguz FINDIK, Karabük University

Prof.Dr. Touhid BHUIYAN, Daffodil International University (Member, IEEE)

Assoc.Prof.Dr. Enver ÖZDEMİR, Istanbul Technical University

Assoc.Prof.Dr. Hakan KUTUCU, Karabük University

Assoc.Prof.Dr. M. Tahir GÜNEŞER, Karabük University

Dr.Md. Mostafijur Rahman, Green University of Bangladesh

Md. Maruf Hassan, Daffodil International University

Asst.Prof.Dr. Caner ÖZCAN, Karabük University

Asst.Prof.Dr. Cihat ŞEKER, Karabük University

Asst.Prof.Dr. Emrah ÖZKAYNAK, Karabük University

Asst.Prof.Dr. Tarik Adnan ALMOHAMAD, Karabük University

Lect. Fatih GÜLTEKİN, Karabük University

Res.Asst. Betül KARAOĞLAN, Karabük University

Res.Asst. İbrahim Ethem YILMAZ, Karabük University

Res.Asst. İdris KAHRAMAN, Karabük University

Welcome to ICONCS 2023

It is a pleasure for us to offer you Abstracts Book for the 3rd International Conference on Cyber Security and Computer Science ICONCS'23. Our goal was to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and present their latest research results, ideas, developments, and applications about all aspects of cyber security, advanced technologies, computer engineering and science. We decided to organize this event with the encouragement of our colleagues in the hope of transforming the event into a symposium series. Now, ICONCS'23 is honored by the presence of over 100 colleagues from various countries. Our warmest thanks go to all invited speakers, authors, and contributors of ICONCS'23 for accepting our invitation. We hope that you enjoy the symposium and look forward to meeting you again in one of the forthcoming ICONCS event.

Best regards,

Chairman of Conference

İÇİNDEKİLER

Physics Informed Neural Network Solutions In R

Melih Ağraz
Giresun University
Faculty of Science and Literature, Giresun, Turkey
melih.agraz@giresun.edu.tr

Abstract—Deep learning is a powerful machine learning method that uses artificial neural networks to learn complex patterns and relationships from data. Its popularity in this field has also strengthened the so-called Physics Informed Neural Network (PINNs) in the field of applied mathematics, with the approximation of the solution of differential equations with the help of deep learning. PINNs can solve two types of problems: data-driven solution and data-driven discovery. In the data-driven solution, the model parameter is kept constant, and PINNs approximate the hidden solution of the differential equation. On the other hand, in the data-driven discovery, PINNs can learn which parameters best describe the observed data. In the data-driven discovery, PINNs can obtain which lambda parameter best describes the observed data. In this study, data-driven solution and data-driven discovery examples will be given for two different differential equations, using R packages related to the two different solutions. It is seen that, it can handle complex, high-dimensional problems and have the potential to revolutionize the field of applied mathematics in R.

Keywords— *Physics informed neural network, machine learning, differential equations, statistics*

Performance Of Grape Leaves Extract As Green Inhibitor On Corrosion Inhibition Of Mild Steel In Acidic Media

Noor Qasim Atiyah Alsaedi
Department of Electrical Power Techniques Engineering
Alamara University college
Missan, Iraq
noor.qassim@alamarahuc.edu.iq

Qasim jaber yousif
Department of Mechinaical Engineering
Missan oil institute
Missan, Iraq
Qasimjaber30@gmail.com

Elaf Qasim Atiyah Alsaedi
Department of petroluem engineering
Alamara University college
Missan, Iraq
noorqasimat@gmail.com

Ali Al-Hashim
Department of Medical Instrumentation Techniques Engineering
Alamara University college
Missan, Iraq
ali.abdalkarim@alamarahuc.edu.iq

Hussien K.Abdul Zahra
Department of Mechanical Engineering
Missan oil institute
Missan, Iraq
hussein.kareem.abdulzahra@gmail.com

Abstract— **The inhibitive effect of grape leaves Extract (GLE) on mild steel in acidic Media with different temperatures polarization measures and weight loss have been used to investigate. The study obtained that the corrosion rate increases with increasing of acid concentration and the used green inhibitor (GLE) inhibited the electrochemical reaction to its lowest levels. Temperature and extract concentration both increase corrosion inhibition effectiveness. Grape leaf extract was adsorbed according to the Langmuir adsorption isotherm. According to the thermodynamic characteristics, there was an exothermic, spontaneous adsorption process with a rise in entropy. Polarization curves demonstrated the mixed-type inhibitory properties of grape leaves extract.**

Keywords— corrosion; mild steel; green inhibitor; grape leaves extract; acidic corrosion.

A Hybrid Security Approach to Nuclear Power Plants

Ebutalha CAMADAN
National Defence University
Ankara, Türkiye
ecamadan@kho.msu.edu.tr
ORCID: 0000-0001-7669-5601

Beste DESTİCİOĞLU TAŞDEMİR
National Defence University
Ankara, Türkiye
bdesticioglu@kho.msu.edu.tr
ORCID: 0000-0001-8321-4554

Fikret BAYKALI
National Defence University
Ankara, Türkiye
fbaykali@kho.msu.edu.tr
ORCID: 0000-0001-7518-8851

Abstract— **It has recently been observed that the energy crisis in the countries has become more severe as a result of the experienced global crises. Similarly, in response to the rising demand for energy, countries have started to use alternative energy sources. Nuclear power plants are regarded as one of the best alternatives for producing energy, in part due to their high energy output and low carbon emissions. However, there are significant adverse effects on both human and environmental health from a potential radioactive leak. Hence, in order to produce nuclear energy safely, the necessary safety precautions should be taken. Providing cyber security has grown in importance as a result of the advancement of technology, both in nuclear power plants and other areas. The 2010 STUXNET attack is an illustration of how challenging and crucial it is to implement the necessary security measures against cyberattacks in nuclear power plants. It has been determined from studies in the literature that there are studies that look at environmental, occupational health and safety, and cyber security concerns separately in nuclear power plants, but that there isn't a study that appears at these issues simultaneously and comprehensively. In order to follow the studies on environmental safety, occupational health and safety, and cyber security in nuclear power plants in an integrated manner, a hybrid safety and security unit approach has been proposed in this study. Additionally, this research will examine the precautions that should be taken in a nuclear power plant for environmental safety, occupational health and safety, and especially cyber security.**

Keywords—cyber security, occupational health safety, nuclear security, nuclear power plants

Analysis of Penetration Testing Standards and Methodologies

Aykhan Huseynli
Uskudar University
Istanbul, Turkey
aykhan.huseynli@st.uskudar.edu.tr

Abstract— **Recently the topic of information security of crucial infrastructure objects became significant to both small companies and large corporations. During the audits, the assessment of an organization's information security policies and the degree of their compliance with the security standards are often checked. However, this approach does not reveal the resilience of the system towards the attacks from malicious actors. To measure to what extent, the system is resilient to attack, penetration tests are held. The purpose of this research is to analyze the existing testing standard and methodologies. The research includes the analysis of methodologies such as OSSTMM, ISSAF, OWASP, PTES, NIST SP 800-115, BSI, PETA, and PTF. Furthermore, the paper discusses the advantages, disadvantages, and focus areas of each methodology.**

Keywords— *IT Security, Penetration Testing, Methodology, IT Security Audit.*

.

The Classification Of Pen Ink Aging By Machine Learning And Deep Learning Technique Using Raman Spectrum

Kübra GÜRBÜZ GÖÇMEN
Engineering Faculty
Istanbul Ticaret University
Istanbul/Turkey
kubra.gocmen@istanbulticaret.edu.tr

Mustafa Cem KASAPBAŞI
Engineering Faculty
Istanbul Ticaret University
Istanbul/Turkey
mckasapbasi@ticaret.edu.tr

Sinan BOSNA
Physics Engineer
Tübitak Bilgem
Kocaeli/Turkey
sinan.bosna@tubitak.gov.tr

Abstract—Forgery of valuable documents generally constitutes falsification methods based on altering a previously written document by using similar or identical ink. In the event of the aforementioned situation, forensic science experts conduct various technical examinations on the relevant document using different devices. One of the main purposes of these examinations is to determine the differences in the aging levels of the inks relative to each other. Raman Spectra, which is also used for different purposes in forensic sciences, is one of the methods that can be used in this field. The Raman spectrometer provides information about molecules' vibration energy levels and presents the analyzed region's spectral signature values. Experts can observe the time-dependent changes that occur in the substances in the region under investigation relative to each other and in the substance content through the information obtained. Utilizing this information, sample data were created at different times using the same pen on A4 paper in our study. These data were divided into two groups old and new data. Raman spectra were taken with a 785 nm laser on both sample data. Sequential Keras model, KNN, and SVM algorithms were used to detect ink aging on paper. The k-fold cross-validation method was used to determine the classification performance more accurately. The results showed that the classification performance was 98.71% for the neural network and 100% for the KNN and SVM.

Keywords—Raman spectroscopy, pen ink, machine learning ,deep learning

A Web Scraping App for Smart Literature Search of the Keywords

Muhammed Ali Mutlu
Analytics Directorate
NTT DATA Business Solutions Turkey
Istanbul, Turkey
muhammed.mutlu@nttdata.com

Eyup Emre Ulku
Faculty of Technology
Marmara University
Istanbul, Turkey
emre.ulku@marmara.edu.tr

Kazim Yildiz
Faculty of Technology
Marmara University
Istanbul, Turkey
kazim.yildiz@marmara.edu.tr

Abstract—Literature review has an important role in the success of long-term studies such as projects, articles and thesis. Search engines provide significant convenience to research processes. However, carrying out comprehensive and systematic research on the web requires a long working process. Various libraries and development tools have been developed and presented in order to perform the literature search processes more efficient, easier, faster and more comprehensive. By using these provided development tools, research processes that may take days can be reduced to hours or even minutes. Literature review is not only needed for academic studies. It is a process that should be applied and performed first in every field where innovative steps are taken. Literature review is a process that gives us important ideas about whether similar studies have been done before, which methods have been used before, and what has not been addressed in previous studies. In addition, it is very important to avoid any copyright problems in the studies to be done. The main purpose of this study is to present an application that will enable the literature review processes to be carried out easier, faster and more efficiently. In current systems, literature search is done by browsing through search websites or various article sites one by one and using the search tools provided by these sites. With the application developed within the scope of this study, an application that is easy to use, enables scanning of the entire WWW environment and presents the scanning results to the user quickly has been revealed.

Keywords— Web Scraping, Web Crawling, Smart Literature Search, Literature Search Framework, Scraping and Crawling Bots

Recognition of Traditional Turkish Cuisine with Convolutional Neural Network

1st Seda KIRTAY
Software Engineering
Istanbul Health and Technology University
Istanbul, Turkiye
0000-0003-2415-9131

2nd Kazım YILDIZ
Computer Engineering
Marmara University
Istanbul, Turkiye
0000-0001-6999-1410

Abstract— **Object recognition and scene classification, which are among the basic and challenging problems of computer vision, have been used in different applications in various fields for many years. The studies carried out in order to enable computers to automatically perceive, recognize, label and classify the content of visuals, which are inherent to human beings, constitute an important field of study in deep learning. The development and combination of this ability with the ever-increasing computational capacity is expected to enable computer vision to realize various applications that are currently unsolvable. In this context, the purpose of this research is to conduct scene recognition of Turkish cuisine flavours using a deep learning convolutional neural network structure. In this context, the recognition process on the scene with a data set of 23 traditional Turkish cuisine flavours was performed with a convolutional neural network and an accuracy of 98.018% was obtained.**

Keywords— Object recognition, Deep learning, Convolutional Neural Network, CNN

Metastasis Prediction with Superlearner Method for Breast Cancer Patient under Different Feature Selection Algorithms

Melih Ağraz
Giresun University
Faculty of Science and Literature, Giresun, Turkey
melih.agraz@giresun.edu.tr

Abstract—Breast cancer is an important and fatal disease, especially seen in women. Detection of metastasis in breast cancer is one of the important steps in preventing the progression of the disease. Super Learning is a stacking ensemble method that uses cross-validated risk to test the performance of the best-weighted model. van der Laan proved in 2007 that this method asymptotically performs as accurately as the best algorithm compared to any single candidate learner algorithm. In this study, microarray metastasis data obtained from 490 female breast cancer patients were modeled with the Superlearner method, and the most important model was determined by applying three differentmachine-learning methods. Before that, Boruta, SVM-RFE and random forest (RF) feature selection (FS) methods were applied to select most appropriate arrays. The most effective metastasis prediction model was obtained with the appropriate features. Accordingly, RF is found to be the best FS method with the highest AUC: 0.688 for Superlearner metastasis prediction model.

Keywords— Ensemble learning, superlearner, machine learning, microarray data

Load Balancing Algorithms in Parallel and Distributed Systems

Ayşe Nur ALTINTAŞ TAKÜL
Computer Engineering Department
Karabuk University
Karabuk, Turkey
aysenuraltintas@karabuk.edu.tr

Saliha ÖZGÜNGÖR
Software Engineering Department
Karabuk University
Karabuk, Turkey
salihaozgungor@karabuk.edu.tr

Burhan SELÇUK
Computer Engineering Department
Karabuk University
Karabuk, Turkey
bselcuk@karabuk.edu.tr

Abstract— In the world, many complex, interrelated events occur simultaneously, in a time-dependent sequence. Compared to serial computing, parallel computing is much more suitable for modeling, simulating and understanding complex real-world events. Modern computers, even laptops, are parallel in architecture with multiple processors/cores. Many problems are so large and/or complex that it is impractical or impossible to solve them on a single computer, especially given the limited computer memory. In its simplest definition, a distributed system is a group of computers that work together to appear as a single computer to the end user. Each has its own local memory and individuals communicate with each other by passing messages. Load balancing is one of the central issues that needs to be resolved to get high performance from a parallel and distributed systems. Load balancing for parallel applications tries to distribute the computational load to as evenly number of processors or machines as possible. The process of distributing or redistributing the load among these processor increases system performance to get highest possible operating speed, optimizing resource usage by fairly distributing computations to processors leads minimizing response time while maximizing throughput. It also aims to prevent overloading of any resource. Since load imbalance directly leads to processor idle times, high efficiency can only be achieved if the computational load is evenly balanced between processors thereby minimizing the time to perform all tasks and reducing the idle time of each processor. Without good load distribution strategies and techniques, we cannot aim to achieve good acceleration and good efficiency. In this study, load balancing problem in parallel and distributed systems will be discussed. Detailed information will be given about the algorithms developed in different strategies for the solution of this problem. Algorithms will be compared and inferences will be made in the light of the given information.

Keywords—load balancing, parallel, distributed, algorithms

Data Security Techniques and Comparison of Differential Privacy Techniques in Bioinformatics

Nilgün İncereis
Computer Engineering
Istanbul Okan University
Istanbul Turkey
Distance Education Application and
Research Center
Bartın University
Bartın, Turkey
niincereis@stu.okan.edu.tr
nincereis@bartin.edu.tr
ORCID: 0000-0001-5508-8159

Hilal Çakır
Computer Engineering
Istanbul Okan University
Istanbul, Turkey
hilcakir@stu.okan.edu.tr
ORCID: 0000-0002-5378-7930

Bekir Tevfik Akgün
Computer Engineering
Yeditepe University
Istanbul, Turkey
bekirtevfik.akgun@yeditepe.edu.tr
ORCID: 0000-0002-9726-1340

Abstract—**Bioinformatics data is data containing information about biological systems and processes. This data can include genomic data, proteomic data, metabolic data, and similar data. The processing and analysis of bioinformatics data aims to achieve important goals such as conducting scientific research and improving healthcare systems. Data security of bioinformatics data ensures the security of data during processing and analysis as well as protecting individual privacy. In this study, five of the known techniques for data security in bioinformatics have been studied. These techniques include: data anonymization, data masking, data encryption, and role-based access control, and differential privacy. In this study, it is aimed to create functions for the above-mentioned data security techniques by using the dataset obtained from 1000 patients with lung cancer, and to anonymize the dataset by using Laplacian, Gaussian and Exponential mechanisms from differential privacy techniques. Looking at various comparison parameters from the differential privacy techniques, it is concluded that the Laplacian technique strikes the best balance between privacy and utility as it provides the highest privacy guarantee and accuracy, as well as the lowest noise and robustness.**

Keywords— Bioinformatics, data security, data anonymization, data masking, data encryption, role-based access control, differential privacy.

Using ANFIS to Predicte the Long and Short Term Stroke Risk Based on Ultrasound Carotid Imaging and Clinical data of Initially Asymptomatic Patients

Suhail Odeh
dept. of Software Engineering
Bethlehem University
Bethlehem, Palestine
sodeh@bethlehem.edu

Efthyvoulos Kyriacou
dept. of Computer Science and
Engineering
Frederick University
Lemesos,, Cyprus
e.kyriacou@frederick.ac.cy

Constantinos S. Pattichis
dept. of Computer Science
University of Cyprus
Nicosia, Cyprus
pattichi@ucy.ac.cy

Abstract—The aim of this study is to investigate the development of predictive modelling in order to estimate the short (less or equal to three years) or long term (more than three years) stroke risk of patients with asymptomatic carotid artery stenosis. Data were collected from 108 patients that had a stroke event have been used. The prediction is done using base line data where patients were still asymptomatic. The information collected includes non-invasive ultrasound images of the carotid arteries and several other clinical data like patient's blood tests (Cholesterol, creatinine, general blood parameters), diabetes, smoking, family history. Ultrasound images were analyzed and several features that can be used in order to characterize the type, size, structure and morphology of the atherosclerotic plaques where extracted. Based on the extracted image features and clinical data; we had created a risk modelling system based on Adaptive Network based Fuzzy Inference System (ANFIS). Model was investigated to classify the subjects into the two classes i) short (≤3 years) and ii) long term (>3 years) period stroke events. The ANFIS could give us correct classification rate up to 97±2.6%. These results can clearly indicate that ultrasound image plaque characteristics in combination with clinical data can be used in order to create predictive models for stroke risk period.

Keywords— *Adaptive Network based Fuzzy Inference System (ANFIS), stroke risk, Feature Selection.*

Coverage Guided Fuzzing for Efficient Performance Profiling: A Low Overhead Method

Berk Cem Göksel
Computer Engineering
TOBB University of Economics and Technology
Lemesos,, Cyprus
b.goksel@etu.edu.tr

Abstract— **Benchmarking large scale software projects is generally done by writing tests for specific modules and/or functions, and getting various performance metrics over repeated iterations. The problem with this approach is that the tests have to be manually written to cover as many of the control flows of the program as possible. This is not a scalable solution, especially for most large scale projects. Coverage guided fuzzing provides a measurable and scalable way of testing a program while covering as many execution states as possible in a much more efficient manner. At present, there is little work on getting performance profiling information while fuzzing a program without introducing significant overhead, which reduces the efficacy of fuzzing. This paper proposes a method which provides a low overhead procedure to utilize coverage guided fuzzing in order to collect performance profiling information.**

Keywords— **Coverage guided fuzzing, performance profiling, eBPF.**

.

A Short Review: Cyber Attacks And Detection Methods Based On Machine Learning And Deep Learning Approaches In Smart Grids

Mehmet KARAYEL
Computer Engineering
Kocaeli University
Kocaeli, Türkiye
226112004@kocaeli.edu.tr

Nevcihan DURU
Faculty of Engineering and Natural Sciences
Kocaeli Health and Technology University
Kocaeli, Türkiye
nevcihan.duru@kocaelisaglik.edu.tr

Mehmet KARA
Faculty of Engineering and Natural Sciences
Kocaeli Health and Technology University
Kocaeli, Türkiye
0000-0001-7312-0503

Abstract—**Power systems and smart grids constitute critical instruments of national security and the economy. In case of the power system malfunctioning, millions of people are affected. Furthermore, there are extreme financial losses, irreversible data casualties and service outages. Recently, the use of commercial smart measuring and control devices in the field of electricity and power systems has become widespread due to the development of applicable technologies and the reduction of the costs of devices. Although this situation has increased traceability and manageability, it also made smart grids more vulnerable to cyber threats compared to the traditional power systems used before. Cyber threats in smart grids are generally categorized as eavesdropping the data to possess detailed information about the system, tampering with data to disturb the system's stability, denial of services to block accessibility and injecting malicious software that can cause damage to the system. FDI attack is considered one of the most severe cyber-attack types due to its stealthy. FDI attacks disrupt the entire stabilization of the smart grid gradually. Machine learning and deep learning methods in supervised, semi-supervised and unsupervised domains have been widely used to protect smart grids against cyber threats by assisting conventional bad data detection mechanisms. Successful results have mainly been obtained by deep learning algorithms such as CNN and RNN. These algorithms have been supported with improved feature selection techniques to increase the accuracy of the detection and decrease the computational burden of the models. The purpose of the paper is to briefly summarize and combine the significance of smart grids, vulnerabilities of smart grids, cyber threats to smart grids, deep learning and machine learning methods applied against cyber-attacks, especially FDI attacks considered to be the most dangerous attack type and potential future research areas.**

Keywords—Power Systems, Smart Grids, Cyber Attack, False Data Injection Attack, FDIA, Machine Learning, Deep Learning, CNN, RNN, LSTM.

A Quantum Machine Learning Approach for Detecting User Locations

Erkan Güler
Department of Computer Engineering
Giresun University
Giresun, Türkiye
erkan.guler@giresun.edu.tr

Muhammet Talha Kakız
Department of Computer Engineering
Osmaniye Korkut Ata University
Osmaniye, Türkiye
mtalhakakiz@osmaniye.edu.tr

Tuğrul Çavdar
Department of Computer Engineering
Karadeniz Technical University
Trabzon, Türkiye
ulduz@ktu.edu.tr

Faruk Baturalp Günay
Department of Computer Engineering
Atatürk University
Erzurum, Türkiye
baturalp@atauni.edu.tr

Burcu Şanal
Vocational School of Technical Sciences
Recep Tayyip Erdoğan University
Rize, Türkiye
burcu.sanal@erdogan.edu.tr

Abstract—Quantum Machine Learning methods are becoming a key component for various types of tasks making predictions or decisions based on datasets. Recent efforts and researches on quantum computing point out the significance of quantum speedup advantage, especially for learning processes that require enormous amount of computational resources. Advances in both quantum hardware design and hybrid quantum-classical software frameworks accommodate a paradigm shift from classical to quantum. In consideration with this quantum leap notion, we investigate the capability of variational quantum algorithms (VQA) on a real world problem of user localization dealing with the binary classification task. This paper introduces a VQA with four variants that differ in the number of layers related to the variational quantum circuit (VQC) part of the VQA. The samples from a publicly available user localization dataset are first preprocessed through padding, scaling and normalization. Next, they are mapped into three qubit quantum states using amplitude encoding as a data embedding scheme. Unitary transformation of the mapped quantum data in the VQC is followed by a measurement in computational basis to produce predictions for the labels. The error between true and predicted labels is computed in a classical manner and a cost function minimization process is executed with the aid of gradient descent algorithm. The updated training parameters from the optimization stage are fed into the VQC and this process is repeated until the learnable parameters converge. The simulation results demonstrate that the designed VQA for binary classification achieves an accuracy value of 99% in the training phase. Moreover, the ratio of predicted labels to true labels approaches to 93% during the validation of actual user locations based on the signal strength received from the routers that are positioned at different places in a facility.

Keywords—quantum machine learning, user localization, variational quantum algorithm, variational quantum circuit, amplitude encoding

SpectreTest: Demonstrating the Hardware-Based Security Attack in Software

Zeki Şahbaz
Electrical Computer Engineering
Abdullah Gul University
Kayseri, TURKEY
zeki.sahbaz@agu.edu.tr

İkram Halıcı
Electrical Computer Engineering
Abdullah Gul University
Kayseri, TURKEY
ikram.halici@agu.edu.tr

Gulay Yalcin
Computer Engineering Department
Abdullah Gul university
Kayseri, TURKEY
gulay.yalcin@agu.edu.tr

Abstract— The design adopted to meet the increasing speed demands in hardware has caused serious problems in terms of security. Branch prediction is a technique used to increase the performance of modern processors, but it also introduces a trade-off between performance and security. Vulnerabilities can arise when using branch prediction, one of which is the Spectre attack. This attack uses side channels to leak data from the cache, allowing privileged data to be accessed from memory.

CPUs try to maintain high performance by using caches inside when they need data from the main memory. Instead of getting the data from the main memory, they keep the data in caches, and when they want to use it again, they quickly access the data from caches. Besides, CPUs use branch prediction to predict the execution direction and speculative execution is carried out in the predicted direction. When the branching direction depends on data from memory, CPUs predict the direction and the speculative execution is performed. The direction of the execution eventually is determined, if it is true, significant performance gain is obtained but otherwise, CPU reverts all changes except that cache changes. Spectre uses this speculative execution adversely and it exploits cache content by using side channels. In our presentation, we have set up two Docker instances to demonstrate this vulnerability. We aim to show that it is possible to read information from one instance by attacking another instance, even if they are running the same server and using the same memory. This highlights the importance of understanding the potential security risks associated with branch prediction and the need to consider these risks when implementing these performance-enhancing features. Our results also demonstrate that increasing the security of one instance alone is not enough in Docker environments where multiple instances share the same resources.

Keywords—hardware security, spectre , simulation, virtual memory

Blockchain-based Privacy Preserving Linear Regression

Zeynep Delal Mutlu
Dept. of Computer Engineering,
TOBB University
Ankara, Turkey
zmutlu@etu.edu.tr

Yesem Kurt Peker
TSTS School of Computer Science,
Columbus State University
Columbus, GA, USA
peker_yesem@columbusstate.edu

Ali Aydın Selçuk
Dept. of Computer Engineering,
TOBB University
Ankara, Turkey
aselcuk@etu.edu.tr

Abstract—**In this study we propose a blockchain-based architecture that uses smart contracts and homomorphic encryption to allow statistical computations on confidential data by third parties. The use of blockchain provides the much-desired security properties of integrity and fault tolerance and homomorphic encryption preserves the privacy of the data. We present the design, implementation, and testing of our system. Our results show that a blockchain-based data sharing mechanism with homomorphic calculations via a smart contract is feasible and provides improvements in protecting the data from unauthorized users. Even though our work focused on linear regression, the architecture can be used for other statistical analysis and machine learning algorithms.**

Keywords—*blockchain, homomorphic encryption, statistics, linear regression, ethereum*

Methods for Increasing the Cyber Resilience of Critical Infrastructures

Fatih Furkan Bayar
Cyber Security Directorate
HAVELSAN
Ankara, Turkey
fbayar@havelsan.com.tr

Sila Sibil Bardak
Cyber Security Directorate
HAVELSAN
Ankara, Turkey
ssibil@havelsan.com.tr

Ender Saribay
Cyber Security Directorate
HAVELSAN
Ankara, Turkey
esaribay@havelsan.com.tr

Ozmen Emre Demirkol, Ph.D.
Cyber Security Directorate
HAVELSAN
Ankara, Turkey
oedemirkol@havelsan.com.tr

Mert Ozarar, Ph.D.
Cyber Security Directorate
HAVELSAN
Ankara, Turkey
mozarar@havelsan.com.tr

Abstract— **Cybersecurity is a critical topic that has become increasingly important in today's world, due to the increasing dependency on technology and interconnected systems. As digitalization increases, the need for cybersecurity measures becomes even more important for several systems that are crucial for society, nuclear facilities, energy systems, finance transportation and healthcare systems. Any damage to critical infrastructures from inside or outside will lead to the deterioration of the social order of countries, the loss of international reputation and the undermining of their credibility. The integration of information technology (IT) and operational technology (OT) within industrial control systems (ICS) has resulted in an expanding attack surface for cyber threats. In order to establish complete cyber-defence solution, innovative artificial intelligence solutions must be utilized alongside traditional cyber security approaches. In the digital transformation process of countries and organizations, the increasing cyber threats are addressed by explaining the five crucial solutions needed, based on international standards. This study aims to provide an overview of strategies to enhance the cyber security maturity level of critical infrastructures, examines both traditional cyber security approaches and artificial intelligence approaches. An architecture is specified to build cyber resilient critical infrastructures.**

Keywords—Critical Infrastructure, Operational Technology, Industrial Control Systems, Cyber Resilience, Artificial Intelligence

Enhancing Zero-Shot Learning Based Sign Language Recognition Through Hand Landmarks And Data Augmentation

Giray Sercan ÖZCAN
Department of Computer Engineering
Baskent University
Ankara, Turkey
gozcan@baskent.edu.tr

Emre SÜMER
Department of Computer Engineering
Baskent University
Ankara, Turkey
esumer@baskent.edu.tr

Yunus Can BİLGE
Image and Video Processing Group
HAVELSAN
Ankara, Turkey
ycbilge@havelsan.com.tr

Abstract— **Sign language recognition remains a challenging area and may require a considerable amount of data to obtain satisfactory results. To overcome this, we use readily available motion text data in addition to videos for achieving recognition of unobserved classes during the training phase. Zero-Shot Sign Language Recognition (ZSSLR) with a novel technique is focused on this work, which learns a model from seen sign classes and recognizes unseen sign classes. To achieve this, the ASL-Text dataset is used which combines the video of word signs and descriptions in sign language dictionaries. Moreover, this dataset consists of sign language classes and their corresponding definitions in the sign language dictionary. In various Zero-Shot Learning (ZSL) applications, it is common for datasets to contain a limited number of examples for numerous classes across different domains. This makes the problem of sign language recognition extremely challenging. We try to overcome this by using a new approach which includes augmented data and hand landmarks. The experiment on augmented data resulted in 50.91 for top-5 accuracy. Hand landmarks are used with unaugmented data which is applied to average and LSTM deep learning layers resulting in 49.41 and 48.21 for top-5 accuracies, respectively.**

Keywords—sign language recognition, zero-shot learning

Medical Diagnosis Support System For Cardiovascular Disease Prediction Machine Learning Based

1st Nidhal Mohsin Hazzaa
Computer Science Dept.
College of Computer Science and Information Technology,
Kirkuk University, Kirkuk, Iraq
Computer Science Dep.
Informatics Institute, Gazi University
Ankara, Turkey
nmohsin.hazzaa@gazi.edu.tr

2nd Oktay Yıldız
Computer Engineering Dept.
Faculty of Engineering, Gazi University
Ankara, Turkey
oyildiz@gazi.edu.tr

Abstract— Early prediction and diagnosis of CVD are crucial for the effective management and prevention of advanced cases. In this study, a diagnosis system using supervised machine learning is proposed to predict CVD. The system employs multiple ML classifiers, including RF, DT, SVM, LR, and MLP, for predicting atherosclerosis. The UCI repository Sani Z-Alizadeh dataset was used for this research. The imbalanced nature of the dataset, which refers to the number of instances belonging to one class being significantly greater than the number of instances belonging to another class, was addressed using the Synthetic Minority Oversampling Technique (SMOTE) for data resampling. Ten-fold cross-validation procedures were used to split the dataset. The performance of the five machine learning (ML) classifiers was evaluated using standard performance metrics. The evaluation revealed that all classifiers achieved a performance improvement of at least 2%. The proposed model has potential applications in healthcare and can improve clinical diagnosis of CVD disorders, leading to optimized diagnosis, prevention of advanced cases, and lower treatment expenses.

Keywords— Heart disease, Medical Diagnosis Support System (MDSS), Clinical data, Machine learning.

A Secure Lightweight Authentication Scheme for RFID Systems in IoT Environment.

Dr. Md. Monzur Morshe,

Daffodil International Univerrsity(Lien from University of Dhaka), Dhaka, Bangladesh , mmmorshed@du.ac.bd

Hongnian Yu,
Edinburgh Napier University,
hongnianyu@uic.edu.cn.

Anthony S. Atkins
Staffordshire University, Stafford, UK,
a.s.atkins@staffs.ac.uk.

Abstract— **Radio Frequency Identification (RFID) technology is suitable for IoT applications. RFID is cheap and light weight and hence it is very popular in IoT technology. The concern of research community is the privacy and security issue of RFID system. Due to low storages of RID tag it a challenging research problem to ensure privacy and security such as data visibility, loss, modification, eavesdrop etc. In this paper we propose a new RFID authentication protocol for RFID system. It ensures privacy and security in IOT environment in a more efficient way. To ensure better security we use a different password for each tag and it changes after each authentication process. It also can protect from an unexpected lack of synchronization in case an incomplete authentication is held for any unwanted problem in authentication phase. The proposed protocol shows some relatively superior performance in some aspects of computation and storages.**

Keywords- RFID security, IoT, privacy, recovery, authentication.

Physical Tracking of ESP32 IoT Devices with RSSI Based Indoor Position Calculation

Özlem Şeker
Department of Computer Engineering
Graduate School of Natural and Applied Sciences
Dokuz Eylul University
Izmir, Turkey
ozlem.yerlikaya@cs.deu.edu.tr

Batuhan Şahin
Department of Computer Engineering
Dokuz Eylul University
Izmir, Turkey
batuhan.sahin@ceng.deu.edu.tr

Tunahan Akdoğan
Department of Computer Engineering
Dokuz Eylul University
Izmir, Turkey
tunahan.akdogan@ceng.deu.edu.tr

Gökhan Dalkılıç
Department of Computer Engineering
Dokuz Eylul University
Izmir, Turkey
dalkilic@cs.deu.edu.tr

Abstract— In recent days, the increase in the number of devices that can access the Internet and the variety of areas where it is used have made it essential to ensure the security of the transmitted data. The unique values embedded in the hardware can be used as keys or secret values within cryptographic algorithms to provide the confidentiality and integrity of the data. In such a situation, maintaining the security of the Internet of things (IoT) device used is a prominent element as well as the privacy of the data. The security requirement of each IoT application may be different. While some applications contain sensitive personal or commercial information, for some applications only the presence of the device may be important. In addition, it is likely to have different devices capable of processing cryptographic algorithms. Within the scope of this study, the distance information was calculated with received signal strength indication (RSSI) data based on 4 reference points of the ESP32 IoT device located indoors. The error rate was observed with the positioning based on the RSSI information of the current position of the device. It has been tested whether it is possible to detect whether the device that transfers the data is legitimate or not via indoor position calculation using RSSI.

Keywords— indoor localization, IoT, RSSI, ESP32, Wi-Fi.

Interaction Between Blockchain Technology and Conventional Databases: a Systematic Literature Review

1st Ahmet Anıl DÜNDAR
Department of Research
and Development
ASELSAN Corporation
Ankara, Turkey
aadundar@aselsan.com.tr

2nd Saim Buğrahan ÖZTÜRK
Department of Research
and Development
ASELSAN Corporation
Ankara, Turkey
sbozturk@aselsan.com.tr

3rd Hakan MUTLU
Department of Research
and Development
ASELSAN Corporation
Ankara, Turkey
hakanmutlu@aselsan.com.tr

Abstract—**Day by day, the popularity of blockchain technology is rising in the business sector. Companies that want to benefit from some of the features of blockchain like security, immutability, decentralization, and elimination of central authority, try to integrate this technology to their existing business use cases. During the integration process, companies must go over a decision process and decide whether the blockchain technology should replace the current system or the two systems should be combined. In order to successfully make the decision, developers or researchers must be aware of the blockchain's features and analyze the improvements that a change between databases and blockchain technology would bring to the existing system. In this paper, in order to provide an outline of differences between blockchain and databases and also ease the decision process that researchers or developers must undergo, we conduct a systematic literature review on the differences between blockchain and databases and possible features they would provide in a system.**

Keywords— Blockchain vs Database, Blockchain Database, Systematic Literature Review

Single Multiplicative Neuron Model in Physics Informed Neural Networks (PINNs)

Melih Ağraz

Giresun University

Faculty of Science and Literature, Giresun, Turkey

melih.agraz@giresun.edu.tr

Abstract— **Machine learning is one of today's popular fields of study, as it gives effective results in subjects such as estimation and classification. Artificial neural networks (ANN) is one of the most effective methods of machine learning. Physics-informed neural network (PINNs) solves physics problems defined through differential equations by including boundary and initial conditions in the loss function of ANN. The most important problem of ANN is to decide the number of neurons and the number of layers, known as the architecture selection problem. The multiplicative neuron model (MNM) is the model in which there is only one neuron in the hidden layer and the aggregate function is multiplicative. The MNM method finds a solution to the architecture selection problem by proposing singular multiplication aggregate function. In this study, we propose the MNM method for the architectural selection problems in the PINNs method. We tested the accuracy of our suggestion in solving the y'-y=0 (for boundaries y(0)=1 and y(1)=e)) equation and found that our proposed method approaches the solution exactly as it does in real PINNs. In addition, we found that our proposed method is 4 times faster than the real PINNs at 30000 epochs.**

Criminal exploitation of information and communication technologies: Riots

Murad M. Madzhumayev

Department of Criminal Law, Criminal Procedure and Criminalistics of   Law Institute

Peoples' Friendship University of Russia (RUDN University)

murad.mad@outlook.com

Moscow, Russian Federation

Abstract—**The availability, reliability, security of information and telecommunication networks and systems constitute crucial pillars for enhancing standards of living, employment, business and civil society organizations, augmenting their activities and realizing the economic potential of the nation.**

The paper addresses the implications of information and communication technologies (ICTs) in the organization, coordination, and perpetration of violent unrest. With global trends in ICT developments and the digital population of the world in mind, it analyses their significance in certain phases of unrest.

The results and conclusions stated in the article are reached based on philosophical and ideological, general scientific and special scientific methods and approaches of research: dialectical, formal-logical (analysis and synthesis, induction, and deduction), synchronous comparative legal method and others.

An examination of the use of ICTs during a violent riot emphasizes the following variations of their utilization: a) informational interaction, communication, incitement; b) mobilization of crowd; c) organization of riots; d) allocation of roles; e) coordination.

As of today, an imminently significant challenge arises out from the criminal liability of internet service providers. The dissemination of information on the Internet involves, in addition to the author himself, other entities, in particular the owner of the network information resource, the owner of the server, etc.

Accordingly, the liability of ISPs for failure to restrict access to information containing advocacy, incitement, recruitment or other involvement in the commission of acts of mass unrest on the part of Internet users arises only if they are aware of the social danger of not restricting access to such information, anticipate the dangerous consequences of mass unrest as a direct consequence of such failure and, in so doing, knowingly direct their intellectual and physical efforts towards it.

Keywords—information and communication technologies, riots, organization of riots, incitement to riot, intermediary liability, internet service providers, mob assembly.

A GaN-based Power Amplifier Module Design for 5G Base Stations

Burak Berk Türk
Electronics and Comm. Eng. Dept.
İstanbul Technical University
İstanbul, Turkey

Furkan Hürcan
Electrical and Electronics Eng. Dept.
İstanbul Medipol University
İstanbul, Turkey

Hüseyin Şerif Savcı
Electrical and Electronics Eng. Dept.
İstanbul Medipol University
İstanbul, Turkey
hsavci@medipol.edu.tr

Hakan Doğan
Electrical and Electronics Eng. Dept.
İstanbul Medipol University
İstanbul, Turkey

Serkan Şimşek
Electronics and Communication Eng. Dept.
İstanbul Technical University
İstanbul, Turkey

Abstract—**This paper presents a compact Power Amplifier Module (PAM) with class-AB topology designed for new-generation cellular base stations. The center frequency of 3.5GHz PAM is designed to target 5G New Radio (NR) and Long Term Evolution (LTE) bands. The module combines lumped element-based input, output matching networks, and a Gallium Nitride (GaN) High Mobility-Electron Transistor (HEMT) die, making it a hybrid design. The module was designed on a Rogers4003C laminate of 8.5 x 5.2 mm. Full-laminate layout electromagnetic analysis and vendor-supplied compact GaN device models are used in co-simulations to check the design's small signal and large signal behavior. The output power is tuned to 37.1 dBm with 39% power added efficiency(PAE). The transducer power gain is 12.4 dB, while the input and output return losses are -11.7 dB and -6.4 dB, respectively. Besides the small signal stability analysis, the large signal conditions are investigated to ensure unconditional stability up to the maximum oscillation frequency of the device.**

Keywords—Gallium nitride HEMT, LTE band 42, 5G n78, power amplifier module

Sentiment Analysis Using BERT on Amazon Reviews

Tea Bogatinoska
Faculty of computer science and engineering
Ss. Cyril and Methodius University in Skopje
Skopje, Macedonia
bogatinoskatea@gmail.com

Jana Trpkovska
Faculty of computer science and engineering
Ss. Cyril and Methodius University in Skopje
Skopje, Macedonia
trpkovskajana@gmail.com

Tamara Mitrevska
Faculty of computer science and engineering
Ss. Cyril and Methodius University in Skopje
Skopje, Macedonia
mitrevskaat@gmail.com

Georgina Mirceva
Faculty of computer science and engineering
Ss. Cyril and Methodius University in Skopje
Skopje, Macedonia
georgina.mirceva@finki.ukim.mk

Abstract—**With the growth of social medias, blogs, discussion forums, online review sites, etc., major companies have come to realize that being sentiment-aware can help them gain insights into user behavior, track and manage their online presence and image and use that information to boost brand loyalties and advocacy, marketing message, product development, monitor competitive intelligence, etc. In this paper, we focus on the research task for sentiment analysis on Amazon reviews data. We used the BERT-base-cased model from Hugging Face. Some experimental results are presented and discussed in this paper.**

Keywords—deep learning, BERT, sentiment analysis, transformers

.

Document Detection With Machine Learning Algorithms

1st İsa YURDABAKAN
Karabük Üniversites, Bilgisayar Mühendisliği
Karabük, Türkiye
0000-0003-2133-5144

2rd Muhammet ÇAKMAK
Karabük Üniversitesi, Elektrik-Elektronik Mühendisliği
Karabük, Türkiye
0000-0002-3752-6642

3nd Erdi YAVUZ
Ahmet Yesevi Üniversitesi, Yönetim Bilişim Sistemleri
Ankara, Türkiye
0000-0002-4364-3941

Abstract— **In recent years, with the beginning of the information age, the importance of digitization has emerged to increase the cost of paper documents and storage, back up information sources produced as a single copy in printed media, and provide archival protection. Digitization is the transfer of documents, especially on paper, to digital media with OCR. Digitization is the process of converting visual and audio data into digital codes so that they can be processed and stored in a computer, apart from documents on paper.**

Digital transformation is a concept that defines the process of finding solutions to social and sectoral needs with the integration of digital technologies, and accordingly the development and change of workflows and culture. The process of transitioning physical records to digital has emerged by processing the information using a binary number system instead of keeping it in a physical environment. The fact that the limited amount of information that can be stored in physical systems could not respond to the increase in information in sectors such as health, media, and finance has created a need, thus accelerating the digital transition process. Organizations allocate significant resources to the rapidly developing software industry in recent years and want to adapt their digital transformation processes as much as possible.

The process of identifying characters using numeric images is important for archiving data on paper. Machine learning methods are used to classify digitized data quickly and accurately. In this study, the classification was made with the best accuracy rate of the texts on the scanned document with machine learning methods. For this reason, Support Vector Machines (SVM), Extremely Randomized Trees, and Naive Bayes (NB) machine methods were examined. A 98.31932% success rate was obtained using Extremely Randomized Trees as the best algorithm.

Keywords— machine learning, optical character recognition, OCR, document classification

Bot Account Analysis on Social Media with Artificial Intelligence Support on Twitter Example

Refik Söylemez
Department of Computer Engineering
İstanbul Ticaret University
İstanbul, Turkey
refiksoylemez@gmail.com

Ali Boyacı
Department of Computer Engineering
İstanbul Ticaret University
İstanbul, Turkey
aboyaci@ticaret.edu.tr

Abstract— **Twitter has undergone significant changes since its launch in 2006, evolving from a platform that only allowed 140-character messages to one that is used for everything from communication to marketing. Researchers have conducted numerous studies on Twitter data, exploring everything from emotion and influence to political polarization and bot analysis. However, these studies have primarily focused on analyzing bot tweets to combat the spread of false information. The accuracy of these analyses varies depending on the selection of training data used to create the machine learning models. In this study, we investigate the impact of different training data on the accuracy of these models, specifically exploring the effects of randomly selected training data on model performance. By examining this important question, we hope to shed new light on the challenges and opportunities of using machine learning methods to analyze Twitter data**

Keywords—Twitter, machine learning, bot tweet

Facial Expression Recognition and Emotion Detection with CNN methods And SVM Classifiers

Nibras Farooq Alkhaleeli
Department of Computer Engineering
Kocaeli University
Kocaeli, Turkiye
nibrasspro@gmail.com

Yaşar Becerikli
Department of Computer Engineering
Kocaeli University
Kocaeli, Turkiye
ybecerikli@kocaeli.edu.tr

Abstract— **There are different humans in our life. With the different languages and cultures of the human, the involuntary methods of facial and body expression remain the most realistic and honest ways. In this study, we will interpret people's emotions through facial expression. A system for detecting human emotions through facial expressions is proposed, in which we first extract facial features using deep learning methods, (VGG16 and MobileNet v1 of CNN models) and then train an SVM algorithm for emotion classification. The results showed that the properties extracted and classified by SVM are superior to the SoftMax classification method in the algorithms (VGG16, MobileNet v1) are used. We see an increase in accuracy of VGG16+SVM equal 3.07 compared to using the Softmax in VGG16. And the resulting accuracy increases by MobileNet+SVM equal 2.737 compared to MobileNet+Softmax. The second part we propose to model a hybrid neural network from each VGG with MobileNet to extract the features and then classification by SVM algorithm.**

Keywords: ***SVM, CNN, Facial Expressions, DeepLearning, Machine Learning, Classification,*** *Convolutional Neural Network, VGG16, MobileNet.*

Model Training Without Sharing Patient Information Between Hospitals with Federated Learning Architecture (FedduCBA)

1st Büşra BÜYÜKTANIR
Department of Computer Engineering
Faculty Technology, Marmara
University
Maltepe, Istanbul, Turkey
0000-0003-2571-4029

2nd Kazım YILDIZ
Department of Computer Engineering
Faculty Technology, Marmara
University
Maltepe, Istanbul, Turkey
0000-0001-6999-1410

3rd Eyüp Emre ÜLKÜ
Department of Computer Engineering
Faculty Technology, Marmara
University
Maltepe, Istanbul, Turkey
0000-0002-1985-6461

4th Tolga BÜYÜKTANIR
Computer Engineering
Loodos Tech,. R&D Office
Maslak, Istanbul, Turkey
0000-0001-5317-0028

Abstract— **The actual sample number and data diversity obtained from more than one hospital affects the success of the model trained with machine learning algorithms in health. Although data production is high for multi-center hospitals, sharing patient information is legally a crime due to data privacy. Federated Learning architecture has been developed as a solution to the mentioned problem. Federated learning is an up-to-date and open-to-development technology that performs model training in multi-center studies without compromising data security. Within the scope of the study, a unified learning architecture was used to ensure data sharing between hospitals without compromising data privacy. According to the architecture, a model is trained within each hospital from its own data. Trained models are sent to the central hospital. Here the models are combined and the final model is created. In order to measure the success of federated learning, the model was trained in the simulation environment by using the relational classification algorithm called Data Unaware Classification Based on Association. The Acute Inflammations dataset from the UCI data pool was used in model training. The data set is divided into training and test set. The data in the training set were assumed they came from different hospitals and were randomly divided to include an equal number of data. In order to observe the operation performed with other hospital numbers, the number of hospitals was assumed to be two, three, and four. As a result of the experiments, each model gave results with 95% accuracy. Thus, it has been concluded that successful models can be produced in health by providing data confidentiality without compromising patient privacy with a federated learning architecture.**

Keywords— *Federated Learning, data unaware CBA, Information Security, Data Privacy, Acute Inflammations*

Enhancing Adaptive Filters with Particle Swarm Optimization: A Hybrid Algorithm Approach

Muhammed Davud
Department of Software Engineering
İstinye University
Istanbul, Turkiye
0000-0002-6864-2339

Alaa Ali Hameed
Department of Software Engineering
İstinye University
Istanbul, Turkiye
0000-0002-8514-9255

Akthar Jamil
Department of Computer Science
FAST School of Computing
Islamabad, Pakistan
0000-0002-2592-1039

Abstract— **Adaptive filtering (AF) is a well-known and intriguing technique with numerous applications. The LMS adaptive algorithm is often utilized in a wide variety of applications due to its simplicity and ease of implementation. Nevertheless, it is well known that the implementation of the conventional LMS method may result in numerical problems due to overflow and poor performance as a result of potentially endless forecast error. Variants of the LMS algorithm, such as the Leaky LMS (LLMS), Zero-Attracting LLMS (ZA-LLMS), Reweighted ZeroAttracting LLMS (RZA-LLMS), Variable Step Size LMS (VSSLMS), Zero-Attracting VSSLMS (ZAVSSLMS), and Reweighted Zero-Attracting VSSLMS (RZAVSSLMS), have been introduced in the literature. In this paper, PSO-RZA-LLMS and PSO-RZAVSS-LMS are presented as hybrid algorithms that make use of the Particle Swarm Optimization (PSO) technique. The suggested hybrid algorithms improve adaptive filtering's performance and accelerate the convergence rate to optimal weights. Experiments demonstrate that the suggested algorithms outperform the conventional RZA-LLMS and RZA-VSS-LMS filters with respect to convergence speed and performance.**

Keywords— *Adaptive filtering, Particle Swarm Optimization, LMS, Hybrid Algorithm.*

A Dynamic Annealing Scheme for Optimizing the Parameterless Self-Organizing Map Algorithm

Alaa Ali Hameed
Department of Software Engineering
İstinye University
Istanbul, Turkiye
0000-0002-8514-9255

Abstract— A The neighborhood function determines the rate of change in the neighborhood surrounding the winning neuron. The neighborhood size is defined as the area covered by activated neighboring neurons in proportion to the winning neuron in each learning iteration. The size of the neighborhood steadily shrinks through rough training for ordering with a large neighborhood radius and then fine-tuning with a small radius. It influences the training result of the Improved Parameter-Less Self-Organising Map (PLSOM2) algorithm procedure. One of the major bottlenecks of the PLSOM2 algorithm is the slow ordering time and difficulty in obtaining a proper neighborhood size, which leads to a topological defect during training, such as kinks or warps in the output maps. Increasing the processing time cannot be enough to overcome these issues. In this paper, we propose a novel dynamic neighborhood function to accelerate the convergence process of the PLSOM2 algorithm to achieve the best shape and adaptation of the neighborhood width. The study demonstrates that by improving the neighborhood function of the PLSOM2 algorithm, the map distortion can be suppressed. It has been shown that the proposed method can handle the network size, neighborhood size, and the large dimensional output space. It also adaptively decreases the neighborhood size over time until the algorithm converges. Also, enforce network growth management appropriately and avoid twisting and misconfiguration. An extensive set of experiments are conducted to evaluate the proposed method. Moreover, comparisons are drawn between the proposed PLSOM2 and several SOM versions to investigate how well it is shaped and adapted to offer optimal neighbor function. The experiment was carried out on eight real-world benchmark datasets in terms of topology preservation and mapping quality. The comparison results demonstrated that the derived dynamic neighborhood function confirmed Keywords:PLSOM2; Neighbourhood Size; Learning Behaviours; Dynamic Annealing Scheme improved learning behavior, topology preserved map, and reduced twisting sensitivity compared to other SOM versions.

Keywords— *PLSOM2; Neighbourhood Size; Learning Behaviours; Dynamic Annealing Scheme.*

Driver Behavior Detection Using Intelligent Algorithms

Naif Adulraheem Mahmood Alzeari
Computer Engineering
Kocaeli University
Kocaeli, Turkiye
nf.abho@gmail.com

Yaşar Becerikli
Department of Computer Engineering
Kocaeli University
Kocaeli, Turkiye
ybecerikli@kocaeli.edu.tr

Abstract— **Driving in today's world is a very complicated and dangerous job that requires full attention. All types of behavior, such as (feeling distracted, aggressive, drowsy, irritable, or tired, can divert the driver's attention away from the road). can lead to accidents and injuries. I can tell you that traffic accidents are a serious problem worldwide. Because this incident is increasing in most countries of the world causing many victims. The aim of this project is to employ machine learning (ML) methods to develop a system capable of identifying driver actions and behaviors. Therefore, it is essential to identify risky driving behaviors such as distracted, aggressive, drowsy, irritable, or tired driving. To achieve this goal, we are working on 15 driver behaviors in this project. We have categorized the provided images using various ML models to determine whether the driver is driving safely or engaging in distracting activities or, aggressive, drowsy, irritable, or tired driving. Our approach involves comparing different models such as Linear Discriminant Analysis (LDA) and Principal Component Analysis (PCA) to determine the best one based on the relevant metrics. The results indicate that. That shows higher precision, recall, F1, and accuracy scores with LDA compared to PCA, especially methods Support Vector Machines (SVM), Bootstrap Aggregating (Bagging), and K-Nearest Neighbors (KNN), Also the results indicate that the combination of PCA and LDA can further enhance the performance of many of the models.**

Keywords: **ML models, Distracted, Aggressive, Drowsy, Angry, Fatigue, PCA, LDA**

Academic Advisor: A Prediction of Undergraduates Students Semester Final's Mark with Contextual Feedback Using Machine Learning Approach

Syeda Farjana Shetu
Daffodil International University
Dhaka, Bangladesh
shetu4247@diu.edu.bd

Fatema Tuj Johora
Green University of Bangladesh
Bangladesh
fatema@cse.green.edu.bd

Md. Mehedi Hasan
Daffodil International University
Dhaka, Bangladesh
mehedibinhafiz@gmail.com

Marzan Tasnim Oyshi
Technische Universität
Dresden, Germany
marzan_tasnim.oyshi@tu-dresden.de

Ms. Nazmun Nessa Moon
Daffodil International University
Dhaka, Bangladesh
moon@daffodilvarsity.edu.bd

Abstract— **The aim of this research is to predict undergraduate students' academic performance using machine learning techniques. With the increasing availability of instructional data, there is a growing potential to utilize this information for educational purposes. Machine learning has become a common approach to predicting student performance, which can be beneficial for improving teaching strategies and student outcomes. This study focused on identifying challenges faced by graduate students who have low academic performance, and how their future performance can be predicted using historical data. The dataset used in this study was collected from a reputable academic institution and analyzed using various machine learning algorithms, such as Decision Trees, Random Forests, Support Vector Machines, Gradient Boosters, Linear Regressions, and Neural Network Regressions. The most effective algorithm was used to predict students' final semester grades. Feedback and suggestions for improvement were provided to students based on their predicted grades. The proposed system, named Academic Advisor, acts as a coach or guide for students, displaying their current academic status and providing customized targets to help them achieve better grades. This research can help educators and institutions improve their teaching strategies and enhance students' academic performance by utilizing machine learning techniques.**

Keywords—Data Analysis, Prediction, Machine Learning, Regression Analysis and Suggestion.