12th INTERNATIONAL SYMPOSIUM ON DIGITAL FORENSICS AND SECURITY

SYMPOSIUM PROGRAM AND ABSTRACTS

EDITED BY
PROF. DR. ASAF VAROL
PROF. DR. MURAT KARABATAK
PROF. DR. CIHAN VAROL
ASST. PROF. DR. EVA TUBA

April 29-30, 2024
Trinity University, San Antonio, TX, US
WELCOME NOTE FROM CO-CHAIRS

We would like to express our great pleasure to present you with the proceedings of the 12th International Symposium on Digital Forensics and Security. We have been organizing this symposium every year for 12 years. We are holding this year’s symposium in the United States, hosted by Trinity University in San Antonio.

We first held the ISDFS symposium in 2013 at Firat University, Elazig, Turkey. Later, it was organized at Sam Houston State University (US, 2014), Gazi University (TR, 2015), The University of Arkansas at Little Rock (US, 2016), The University of Medicine, Pharmacy, Sciences and Technology of Tirgu Mures (Romania, 2017), Firat University (TR, 2018), Instituto Politecnico do Cavado e do Ave (PT, 2019), Arab Open University (LB, 2020), Firat University (TR, 2021), Maltepe University (TR, 2022) and The University of Tennessee at Chattanooga (US, 2023), respectively.

Since 2016, ISDFS has been supported technically by IEEE. We have been carrying out this event under the umbrella of the IEEE Education Society since 2023.

In this symposium, we mainly cover digital forensics, cyber security, information security, cryptography, artificial intelligence (AI), and machine learning areas. However, we also include other papers outside these fields that are related to computer science.

This event is carried out with the support of the following consortium members in 2024: Arap Open University (LB), Association of Software and Cyber Security of Turkey, Firat University (TR), Gazi University (TR), Hacettepe University (TR), IEEE Education Society (US), Karadeniz Technical University (TR), Maltepe University (TR), Ondokuz Mayis University (TR), Osmangazi University (TR), Polytechnic Institute of Cavado and Ave (PT), Sam Houston State University (US), Singidunum University (RS), The University of Tennessee at Chattanooga (US), Trinity University (US) and Yildiz Technical University (TR). We would like to thank the consortium members wholeheartedly for their contributions to the event. Moreover, in the scientific committee of the symposium, scientists from many countries of the world carried out their duties as referees of the papers with great care.

This year we have two invited speakers. Prof. Dr. Hamadou Saliah-Hassane from Canada’s TELUQ University will give a speech on “Developing Educational Standards on Secure and Trusted Learning Systems: Opportunity, Progress, and Challenges”. Our other speaker Prof. Dr. Milan Tuba from Singidunum University will give a speech on “Security Issues in Machine Learning Algorithms”.

Interest in the ISDFS symposium increases every year and scientists from different countries participate. This year, we received the highest number of paper submissions and had to make hard decisions to reject some of the work based on the reviewers’ comments. This year we have participants from Australia, Azerbaijan, Brazil, Canada, China, Ecuador, France, Germany, Greece, Ireland, India, Indonesia, Iraq, Italy, Lebanon,
Mexico, Nigeria, Pakistan, Portugal, Qatar, Saudi Arabia, Serbia, Spain, Switzerland, Turkey, United Arab Emirates, the United Kingdom and the United States.

President Prof. Dr. Vanessa B. Beasley and Provost Prof. Dr. Megan Mustain made sure that this event was held at Trinity University. We thank them for their leadership and support. Some of the students in the Department of Computer Science at Trinity University supported this event. We also thank them for their contributions.

Prof. Dr. Cihan Varol and Prof. Dr. Murat Karabatak made significant contributions in all the stages of the organization of this symposium. We thank them for their incredible contributions to us. The contribution of Prof. Dr. Martin Llamas Nistal, Chair of the IEEE Education Society, to the symposium, who has ensured that this symposium has been held under the umbrella of IEEE Education Society for 2023 and 2024, is undeniable.

Sincerely Yours,

April 29th, 2024

Assist. Prof. Dr. Eva Tuba
Term Chair of ISDFS 2024

Prof. Dr. Ahad Nasab
Chair of ISDFS 2024

Prof. Dr. Asaf Varol
General Chair of ISDFS
ORGANIZERS

HONORARY BOARD

Prof. Dr. Vanessa B. Beasley President, Trinity University, US
Prof. Dr. Megan Mustain Provost, Vice President for Academic Affairs, Trinity University, US
Prof. Dr. Steven R. Angle Chancellor, The University of Tennessee at Chattanooga, US
Prof. Dr. Jerold Hale Provost, The University of Tennessee at Chattanooga, US
Prof. Dr. Edibe Sözen Rector of Maltepe University, TR
Prof. Dr. Fahrettin Göktaş Rector of Fırat University, TR
Prof. Dr. Hamdullah Çuvalcı Rector of Karadeniz Technical University

General Chair of ISDFS
Prof. Dr. Asaf Varol University Tennessee at Chattanooga, TN, US

Chair of ISDFS 2024
Prof. Dr. Ahad Nasab University Tennessee at Chattanooga, TN, US

Term Chair of ISDFS 2023
Assist. Prof. Dr. Eva Tuba Trinity University, TX, US

Publication Chair&Treasurer
Prof. Dr. Cihan Varol Sam Houston State University, TX, US

The IEEE Sponsors

Prof. Dr. Martin Llamas Nistal Chair of the IEEE Education Society, SP
Prof. Dr. Mélanie Ciampi da Brito IEEE Education Society Conference Chair, US
Prof. Dr. Hamadou Saliah-Hassane Member of the Administrative Committee of IEEE Education Society

Signatory Person
Prof. Dr. Asaf Varol The University of Tennessee at Chattanooga, TN, US

Technical Program Contacts

Assist. Prof. Dr. Eva Tuba Computer Science, Trinity University, TX, US, Co-Chair
Prof. Dr. Murat Karabatak Fırat University, TR, Co-Chair
Prof. Dr. Hamadou Saliah-Hassane Member of the Administrative Committee of IEEE Education Society

Assoc. Prof. Dr. Songul Karabatak Fırat University, Türkiye
Prof. Dr. Özay Gürtüğ Maltepe University, Istanbul, Türkiye
Assist. Prof. Dr. Serkan Varol The University of Tennessee at Chattanooga, TN, US

Graphic Design
Assist. Prof. Dr. Tamer Kavuran Fırat University, Turkey
Mahmut Kaplan Fırat University, Turkey
**Web Design**
Prof. Dr. Asaf Varol  The University of Tennessee at Chattanooga, TN, US

**Venue Contact**
Assist. Prof. Dr. Eva Tuba  Trinity University, TX, US

**Consortium Members**
Dr. Khouloud Samrouth  Arab Open University, LB
Prof. Dr. Murat Karabatak,  Association of Software and Cyber Security of Türkiye TR
Prof. Dr. Murat Karabatak  Firat University, Elazig, TR
Prof. Dr. Şeref Sarıoğlu  Gazi University, Ankara, TR
Prof. Dr. Çetin Arslan  Hacettepe University, Ankara, TR
Prof. Dr. Özyay Gürtuğ  Maltepe University, Istanbul, TR
Assoc. Prof. Dr. Sedat Akleylek  Ondokuz Mayis University, Samsun, TR
Asst. Prof. Dr. İker Özçelik  Osmangazi University, Eskişehir, TR
Prof. Dr. Maria M. Cruz-Cunha  Polytechnic Institute of Cavado and Ave, PT
Prof. Dr. Cihan Varol  Sam Houston State University, Texas, US
Prof. Dr. Yusuf Öztürk  San Diego State University, San Diego, US
Assist. Prof. Dr. Eva Tuba  Trinity University, US
Prof. Dr. Milan Tuba  Singidunum University, Serbia
Prof. Dr. Hamadou Saliah-Hassane  TELUQ University, Quebec, CA and IEEE Education Society
Prof. Dr. Ahad Nasab  The University of Tennessee at Chattanooga, TN, US
Prof. Dr. Nizamettin Aydın  Yıldız Technical University, Istanbul, TR
Prof. Dr. Martin Llamas Nistal  Chair of the IEEE Education Society, SP
Prof. Dr. Mélanie Ciampi da Brito  IEEE Education Society Conference Chair, BR
Prof. Dr. Gençağa Pürçek  Karadeniz Technical University, TR
<table>
<thead>
<tr>
<th>First Name</th>
<th>Middle</th>
<th>Last Name</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abdulsamet</td>
<td>Hasiloglu</td>
<td></td>
<td>Istanbul Gelişim University, TR</td>
</tr>
<tr>
<td>Ahad</td>
<td></td>
<td>Nasab</td>
<td>The University of Tennessee at Chattanooga, TN, USA</td>
</tr>
<tr>
<td>Ahmet</td>
<td>Çinar</td>
<td></td>
<td>Fırat University, TR</td>
</tr>
<tr>
<td>Ahmet</td>
<td>Furkan</td>
<td>Aydoğan</td>
<td>Sam Houston State University, US</td>
</tr>
<tr>
<td>Aishwarya</td>
<td>Asesh</td>
<td></td>
<td>Adobe</td>
</tr>
<tr>
<td>Ali</td>
<td>Yazici</td>
<td></td>
<td>Atilim University, TR</td>
</tr>
<tr>
<td>António</td>
<td>M. Rosado da Cruz</td>
<td></td>
<td>Instituto Politécnico de Viana do Castelo, PT</td>
</tr>
<tr>
<td>Asaf</td>
<td>Varol</td>
<td></td>
<td>The University of Tennessee at Chattanooga, TN, USA</td>
</tr>
<tr>
<td>Ashar</td>
<td>Neyaz</td>
<td></td>
<td>Wentworth Institute of Technology, USA</td>
</tr>
<tr>
<td>Ashwin</td>
<td>Viswanathan</td>
<td>Kannan</td>
<td>Amazon Labs, USA</td>
</tr>
<tr>
<td>Avinash</td>
<td>Kumar</td>
<td></td>
<td>Sam Houston State University, USA</td>
</tr>
<tr>
<td>Avni</td>
<td>Morgül</td>
<td></td>
<td>Maltepe University, TR</td>
</tr>
<tr>
<td>Ayhan</td>
<td>Osman</td>
<td>Erdem</td>
<td>Gazi University, TR</td>
</tr>
<tr>
<td>Ayşe</td>
<td>Güler</td>
<td></td>
<td>Gazi University, TR</td>
</tr>
<tr>
<td>Ayşe</td>
<td>Salman</td>
<td></td>
<td>Maltepe University, TR</td>
</tr>
<tr>
<td>Aytuğ</td>
<td>Boyacı</td>
<td></td>
<td>National Defense University, TR</td>
</tr>
<tr>
<td>Banu</td>
<td>Diri</td>
<td></td>
<td>Yıldız Technical University, TR</td>
</tr>
<tr>
<td>Bihter</td>
<td>Das</td>
<td></td>
<td>Fırat University, TR</td>
</tr>
<tr>
<td>Bilal</td>
<td>Alatas</td>
<td></td>
<td>Fırat University, TR</td>
</tr>
<tr>
<td>Bisso</td>
<td>Bisso</td>
<td>Saley</td>
<td>Université Abdou Moumouni, NE</td>
</tr>
<tr>
<td>Bartók</td>
<td>Roland</td>
<td></td>
<td>Miskolc-Egyetemváros, HU</td>
</tr>
<tr>
<td>Burcu</td>
<td>Koç</td>
<td></td>
<td>Middle East Technical University, TR</td>
</tr>
<tr>
<td>Cihan</td>
<td>Varol</td>
<td></td>
<td>Sam Houston State University, USA</td>
</tr>
<tr>
<td>Constantino</td>
<td>Martins</td>
<td></td>
<td>Polytechnic of Porto, PT</td>
</tr>
<tr>
<td>Dalei</td>
<td>Wu</td>
<td></td>
<td>The University of Tennessee at Chattanooga, US</td>
</tr>
<tr>
<td>Derya</td>
<td>Avcı</td>
<td></td>
<td>Fırat University, TR</td>
</tr>
<tr>
<td>Ecir</td>
<td>Uğur</td>
<td>Kucuksille</td>
<td>Suleyman Demirel University, TR</td>
</tr>
<tr>
<td>Elif</td>
<td>Altay</td>
<td></td>
<td>Celal Bayar University, TR</td>
</tr>
<tr>
<td>Elio</td>
<td>Sancristobal</td>
<td>Ruiz</td>
<td>UNED, ES</td>
</tr>
<tr>
<td>Emin</td>
<td>Murat</td>
<td>Esin</td>
<td>Maltepe University, TR</td>
</tr>
<tr>
<td>Emre</td>
<td>Olca</td>
<td></td>
<td>Maltepe University, TR</td>
</tr>
<tr>
<td>Ensar</td>
<td>Gül</td>
<td></td>
<td>Maltepe University, TR</td>
</tr>
<tr>
<td>Erdal</td>
<td>Güvenoğlu</td>
<td></td>
<td>Maltepe University, TR</td>
</tr>
<tr>
<td>Erhan</td>
<td>Akbal</td>
<td></td>
<td>Fırat University, TR</td>
</tr>
<tr>
<td>Erkan</td>
<td>Duman</td>
<td></td>
<td>Fırat University, TR</td>
</tr>
<tr>
<td>Erkan</td>
<td>Kaplanoğlu</td>
<td></td>
<td>The University of Tennessee at Chattanooga, TN, USA</td>
</tr>
<tr>
<td>Erkan</td>
<td>Tanyıldızı</td>
<td></td>
<td>Fırat University, TR</td>
</tr>
<tr>
<td>Eşref</td>
<td>Adalı</td>
<td></td>
<td>Istanbul Technical University, TR</td>
</tr>
<tr>
<td>Eva</td>
<td>Tuba</td>
<td></td>
<td>Trinity University, USA</td>
</tr>
<tr>
<td>Fatih</td>
<td>Ozkaynak</td>
<td></td>
<td>Fırat University, TR</td>
</tr>
<tr>
<td>Ferhat</td>
<td>Uçar</td>
<td></td>
<td>Fırat University, TR</td>
</tr>
<tr>
<td>Filiz</td>
<td>Çağatay</td>
<td>Uğgun</td>
<td>Maltepe University, TR</td>
</tr>
<tr>
<td>Gheorghe</td>
<td>Sebestyen</td>
<td></td>
<td>Technical University of Cluj-Napoca, RO</td>
</tr>
<tr>
<td>Gökhlan</td>
<td>Erdemir</td>
<td></td>
<td>The University of Tennessee at Chattanooga, TN, USA</td>
</tr>
<tr>
<td>Hacer</td>
<td>Varol</td>
<td></td>
<td>Stephen F. Austin State University, US</td>
</tr>
<tr>
<td>Hala</td>
<td>Strohmier</td>
<td></td>
<td>University of South Carolina, USA</td>
</tr>
<tr>
<td>Halit</td>
<td>Oğuztüzün</td>
<td></td>
<td>Middle East Technical University, TR</td>
</tr>
<tr>
<td>Halit</td>
<td>Hami</td>
<td>Öz</td>
<td>İstanbul Gelişim University, TR</td>
</tr>
<tr>
<td>Hamadou</td>
<td>Saliah</td>
<td>Hassane</td>
<td>Teluq University, CA</td>
</tr>
<tr>
<td>Hanumat</td>
<td>Sastry</td>
<td></td>
<td>School of Computer Science UPES, IN</td>
</tr>
</tbody>
</table>
Hürevren Kılıç Atılım University, TR
Huseyin Aygün Montgomery College, USA
Ibrahim Sogukpinar Gebze Institute of Technology, TR
Ibrahim Turkoglu Fırat University, TR
İnan Güler Gazi University, TR
Jayesh Soni Florida International University, US
Jennifer Vilaca Polytechnic Institute of Câvado and Ave, PT
Joaquim Santos Polytechnic of Porto – ISEP, PT
Joaquim Silva Polytechnic University of Câvado and Ave, PT
Adnan Barja IMEC & University of Antwerp, BE
Khalid Tantawi The University of Tennessee at Chattanooga, TN, USA
Khalid Zine Mohammed V University in Rabat, FSR, MA
Khushi Gupta Sam Houston State University, USA
Lahcen Tamym Aix-Marseille University, University of Toulon, FR
Lalith Maddali BrightEdge Technologies, US
Lei Zhang University of Maryland Eastern Shore, US
Luis Ferreira Polytechnic Institute of Câvado and Ave, PT
Madhuri Koushik Netflix
Mandar Khoje Moveworks, USA
Manoj Gupta JECRC University, Jaipur, IN
Maria Manuela Cruz Polytechnic Institute of Câvado and Ave, PT
Mehmet Kaya Syracuse University, USA
Muhammet Baykara Fırat University, TR
Miguel Rodriguez Artacho UNED University, ES
Mohammed Abounaima Sidi Mohamed Ben Abdellah University, MA
Muhammed Burak Maltepe University, TR
Muharrem Tolga Trakya University, TR
Murat Aydogan Fırat University, TR
Murat Karabatak Fırat University, TR
Mustafa Kaya Atılım University, TR
Narasimha K. Karpoor Shashidhar Sam Houston State University, USA
Nizamettin Aydın Yıldız Technical University, TR
Nuno Coelho University of Trás os Montes e Alto Douro, PT
Nuno Lopez Polytechnic Institute of Câvado and Ave, PT
Nuno Rodrigues Polytechnic Institute of Câvado and Ave, PT
Ömer Faruk Bay Gazi University, TR
Oruç Raif Önvural Maltepe University, TR
Osman Altay Celal Bayar University, TR
Osman Erdem Gazi University, TR
Ozal Yıldırım Fırat University, TR
Ozay Gürtuğ Maltepe University, TR
Paulo Teixeira Polytechnic University of Cavado and Ave, PT
Pedro Pinto Instituto Politécnico de Viana do Castelo (IPVC), PT
Raul Cordeiro Sharing University, US
Resul Das Fırat University, TR
Rui Silva Instituto Politécnico de Beja, PT
Salah El Hadaj Cadi Ayad University, MA
Salih Kibaroğlu Maltepe University, TR
Salim Jibrin Danbatta Üsküdar University, TR
Sandro Carvalho Polytechnic Institute of Câvado and Ave, PT
Sedat Akleylek Ondokuz Mayıs University, TR
Sengül Dogan Fırat University, TR
Seref Sagiroğlu Gazi University, TR
Serkan Gönen Istanbul Gelişim University, TR
Serkan Varol The University of Tennessee at Chattanooga, TN, USA
<table>
<thead>
<tr>
<th>Name</th>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seong</td>
<td>Dae Kim</td>
<td>The University of Tennessee at Chattanooga, TN, USA</td>
</tr>
<tr>
<td>Sırma</td>
<td>Çekirdek Yavuz</td>
<td>Yıldız Technical University, TR</td>
</tr>
<tr>
<td>Şule</td>
<td>Gündüz Öğütcü</td>
<td>Istanbul Technical University, TR</td>
</tr>
<tr>
<td>Susan</td>
<td>Anwar</td>
<td>Philander Smith College, US</td>
</tr>
<tr>
<td>Taner</td>
<td>Tuncer</td>
<td>Fırat University, TR</td>
</tr>
<tr>
<td>Tolga</td>
<td>Sakallı</td>
<td>Trakya University, TR</td>
</tr>
<tr>
<td>Tuğba</td>
<td>Akyel</td>
<td>Maltepe University, TR</td>
</tr>
<tr>
<td>Tuğba</td>
<td>Dalyan</td>
<td>Istanbul Bilgi University, TR</td>
</tr>
<tr>
<td>Turker</td>
<td>Tuncer</td>
<td>Fırat University, TR</td>
</tr>
<tr>
<td>Ümit</td>
<td>Can</td>
<td>Munzur University, TR</td>
</tr>
<tr>
<td>Volkan</td>
<td>Tunali</td>
<td>University of the West of Scotland</td>
</tr>
<tr>
<td>Wolday</td>
<td>Abrha</td>
<td>The University of Tennessee at Chattanooga, TN, USA</td>
</tr>
<tr>
<td>Yingfeng</td>
<td>Wang</td>
<td>The University of Tennessee at Chattanooga, TN, USA</td>
</tr>
<tr>
<td>Yorgo</td>
<td>Şenikoğlu</td>
<td>Maltepe University, TR</td>
</tr>
<tr>
<td>Yu</td>
<td>Liang</td>
<td>The University of Tennessee at Chattanooga, US</td>
</tr>
<tr>
<td>Yunus</td>
<td>Santur</td>
<td>Fırat University, TR</td>
</tr>
<tr>
<td>Yusuf</td>
<td>Ozturk</td>
<td>San Diego University, USA</td>
</tr>
<tr>
<td>Zisis</td>
<td>Tsiatsikas</td>
<td>University of the Aegean, GR</td>
</tr>
</tbody>
</table>
SYMPOSIUM PROGRAM

VENUE: TRINITY UNIVERSITY, 106 OAKMONT CT, SAN ANTONIO, TX, USA
DIGITAL FORENSICS AND SECURITY SYMPOSIUM (YOUTUBE CHANNEL)

DICKLE HALL 104: CLICK TO JOIN MEETING
DICKLE HALL 108: CLICK TO JOIN MEETING

APRIL 29, 2024 (MONDAY)

09:00-09:45 REGISTRATION

09:45-10:30 OPENING CEREMONY (DICKLE HALL 104 - MABEE AUDITORIUM)

ASSIST. PROF. DR. EVA TUBA, ISDFS 2024 TERM CHAIR
PROF. DR. AHAD NASAB, CO-CHAIR OF ISDFS 2024
PROF. DR. ASAF VAROL, GENERAL CHAIR OF ISDFS
PROF. DR. MARTIN LIAMAS NISTAL, PRESIDENT OF IEEE EDUCATION SOCIETY
PROF. DR. DAVID RIBBLE, DEAN OF THE SCHOOL OF SCIENCE, SCHOOL OF SCIENCE AT TRINITY UNIVERSITY
PROF. DR. FAHRETTIN GÖKTAŞ, RECTOR OF FIRAT UNIVERSITY
PROF. DR. ÖZAY GÜRTÜG, PRESIDENT’S ADVISORY BOARD MEMBER OF MALTEPE UNIVERSITY
PROF. DR. MEGAN MUSTAIN, PROVOST OF TRINITY UNIVERSITY

10:30-11:00 KEYNOTE SPEECH (DICKLE HALL 104 - MABEE AUDITORIUM)

CHAIR: PROF. DR. CIHAN VAROL
SPEAKER: PROF. DR. HAMADOU SALIAH-HASSANE (TELUQ UNIVERSITY)
TITLE: DEVELOPING EDUCATIONAL STANDARDS ON SECURE AND TRUSTED LEARNING SYSTEMS: OPPORTUNITY, PROGRESS AND CHALLENGES

11:30-12:30 SESSION 01 PRESENTATIONS (CHAIR: ASSIST. PROF. DR. EVA TUBA)

DICKLE HALL 104 - MABEE AUDITORIUM (IN PERSON)

PAPER ID 11: ANALYZING CRYPTOCURRENCY SOCIAL MEDIA FOR PRICE FORECASTING AND SCAM DETECTION
LAKSHMI PRIYA KRISHNAN, IMAN VAKILINIA, SANDEEP REDDIVARI, SANJAY AHUJA

PAPER ID 42: OPINIONS EVOLUTION ANALYSIS IN TIME-VARYING SOCIAL NETWORKS: A SILENT SPIRAL OPINION MODEL
SHAN LIU, HANFEI ZHAO

PAPER ID 134: TOWARDS PRIVACY-PRESERVING VEHICLE DIGITAL FORENSICS: A BLOCKCHAIN APPROACH
TRENT MENARD, MAHMOUD ABOUYOUSSEF
PAPER ID 158: CASSAVA PLANT DISEASE DETECTION USING TRANSFER LEARNING WITH CONVOLUTIONAL NEURAL NETWORKS
Julia Alford, Eva Tuba

11:30-12:30 SESSION 02 PRESENTATIONS (CHAIR: DR. YU ZHANG)

DICKE HALL 108 (ONLINE)

PAPER ID 20: ADVERSARIAL MACHINE LEARNING FOR DETECTING ADVANCED THREATS INSPIRED BY STUXNET IN CRITICAL INFRASTRUCTURE NETWORKS
Hafiz Bilal Ahmad, HaiChang Gao, Naila Latif, Abdul Aziiz, Muhammad Auraangzeb, and Muhammad Tanveer Khan

PAPER ID 52: IDENTIFYING MALWARE FAMILY WITH STRING MATCHING ALGORITHMS BASED ON API Calls AND ENTIRE STRINGS
Kubra Gundogdu, Khushi Gupta, Laura J Garland, Cihan Varol, Narasimha K Shashidhar

PAPER ID 80: SECURING HEALTHCARE 5.0: EXPLORING BYOD CYBER RISKS, MISUSE CASES, AND BEST PRACTICES
Durga Srikant Maguluri, Leela Pavani Velagala, Gahangir Hossain

PAPER ID 88: HNMBLOCK: BLOCKCHAIN TECHNOLOGY POWERED HEALTHCARE NETWORK MODEL FOR EPIDEMIOLOGICAL MONITORING, MEDICAL SYSTEMS SECURITY, AND WELLNESS
Naresh Kshetri, Rahul Mishra, Mir Rahman, Tanja Steigner

PAPER ID 138: ALGOXSSF: DETECTION AND ANALYSIS OF CROSS-SITE REQUEST FORGERY (XSRF) AND CROSS-SITE SCRIPTING (XSS) ATTACKS VIA MACHINE LEARNING ALGORITHMS
Naresh Kshetri, Dilip Kumar, James Hutson, Navneet Kaur, Omar Osama

12:30-14:00 LUNCH (DICKE HALL JOHN AND JANICE BRAZIL COMMONS)

14:00-14:30 KEYNOTE SPEECH (DICKE HALL 104 - MABEE AUDITORIUM)
Chair PROF. DR. ASAF VAROL
Speaker PROF. DR. MILAN TUBA (SINGIDUNUM UNIVERSITY)
Title SECURITY ISSUES IN MACHINE LEARNING ALGORITHMS

14:30-16:00 SESSION 03 PRESENTATIONS (CHAIR: DR. HAMADOU SALIHA-HASSANE)
DICKE HALL 104 - MABEE AUDITORIUM (IN PERSON)

PAPER ID 35: ANALYZING INSIDER CYBER THREATS AND HUMAN FACTORS WITHIN THE FRAMEWORK OF AGRICULTURE 5.0
Kossi D Bissadou, Gahangir Hossain, Leela Pavani Velagala, Salleh Sonko

PAPER ID 75: A ROBUST MISBEHAVIOR DETECTION SYSTEM FOR COOPERATIVE DRIVING NETWORK
Abdullahi Modibbo Abdullahi, Wassila Lalouani, Messaoud Rahim

PAPER ID 79: UNRAVELING IOT TRAFFIC PATTERNS: LEVERAGING PRINCIPAL COMPONENT ANALYSIS FOR NETWORK ANOMALY DETECTION AND OPTIMIZATION
Bradley A Boswell, Seth Barrett, Gokila Dorai
PAPER ID 100:  CYBER READY RURAL: UNDERSTANDING LAW ENFORCEMENT CYBER READINESS  
LUCY TSADO, CAMILLE GIBSON, IZZAT ALSMADI, JANAYA BOB

PAPER ID 132:  DECODING DOOH VIEWABILITY USING YOLO FOR PRIVACY-FRIENDLY HUMAN SILHOUETTE IDENTIFICATION ON LiDAR POINT CLOUDS  
ANNA FORSTER, CARLO LUCHERONI, STEFAN GÜRTLER

14:30-16:00  SESSION 04 PRESENTATIONS (CHAIR: DR. SHENG TAN)  
DICKE HALL 108 (ONLINE)

PAPER ID 10:  SDN SECURITY CHANNEL CONSTRUCTED USING SM9  
DAN WANG, LIANGYU DONG, TANG HUA, JUNJIE GU, ZIWEI LIU, XINTONG YOU

PAPER ID 32:  CHAOS-BASED STREAM CIPHERS FOR 5G INTER-SLICE NETWORK SECURITY  
VISMAYA VIJAYAN

PAPER ID 33:  COMPARATIVE ANALYSIS OF AUTOMATED SCANNING AND MANUAL PENETRATION TESTING FOR ENHANCED CYBERSECURITY  
NIKHIL RANE, AMNA QURESHI

PAPER ID 67:  EXPLORING SECURITY, PRIVACY, AND FORENSICS CONCERNS IN THE METAVERSE  
SULTAN ALTHAQEEL, SHEMA ALENAZI, SUMAYA ALSHOKEERAN

PAPER ID 99:  DNS TUNNEL PROBLEM IN CYBERSECURITY  
GÜNEŞ GÜRSOY, ASAF VAROL, AHAD NASAB

PAPER ID 136:  CONTRIBUTION OF ALGORITHM VISUALIZATIONS TO STUDENTS' LEARNING SKILLS: A PEDAGOGICAL APPROACH  
HAREM ALI KHEDER, ASAF VAROL

15:45-16:00  COFFEE BREAK

16:00-18:00  SESSION 05 PRESENTATIONS (CHAIR: DR. HALA STROHMIER)  
DICKE HALL 104 - MABEE AUDITORIUM (IN PERSON)

PAPER ID 87:  SECURITY AND PRIVACY THREATSPOSED BY IOT DEVICES USED BY STUDENTS ON COLLEGE CAMPUSSES  
HALA STROHMIER

PAPER ID 106:  EXAMINATION OF ARTIFICIAL INTELLIGENCE INTEGRATION AND ITS IMPACT IN HIGHER EDUCATION  
HALA STROHMIER

PAPER ID 120:  EFFECT OF SIGNAL CONDITIONING AND EVOKED POTENTIAL BASED REPRESENTATION ON STABILITY AND DISTINCTIVENESS OF EEG BRAIN SIGNATURES  
MUHAMMED E OZTEMEL, OMER SOYSAL

PAPER ID 159:  CREDIBLE DIFFUSION: IMPROVING DIFFUSION MODELS INTERPRETABILITY WITH TRANSFORMER EMBEDDINGS  
MATVEI POPOV, EVA TUBA

X
PAPER ID 160: OPTIMIZING MACHINE LEARNING FOR BREAST CANCER DETECTION BY HYBRID METAHEURISTIC APPROACH
TIMEA BEZDAN, IVANA STRUMBERGER, MILAN TUBA

16:00-18:00 SESSION 06 PRESENTATIONS (CHAIR: DR. MATTHEW HIBBS)
DICKE HALL 108 (ONLINE)

PAPER ID 24: PERFORMANCE COMPARISON ANALYSIS OF DIGITAL FORENSIC TOOLS IN VARIOUS OPERATING SYSTEMS
ATHANASIOS MANIOS, CHRISTOS LIAMBAS

PAPER ID 72: FORENSIC ANALYSIS OF WHATSAPP, INSTAGRAM, AND TELEGRAM ON VIRTUAL ANDROID DEVICE
DINA MILLATINA

PAPER ID 82: STREAM CLUSTERING ON A FORENSIC TIMELINE
DEKA JULIAN ARRIZKI, STEFANUS ALBERT KOSIM, HUDAN STUDIAWAN*

PAPER ID 109: A FRAMEWORK FOR INTEGRATED DIGITAL FORENSIC INVESTIGATION EMPLOYING AUTOGEN AI AGENTS
AKILA SHAMENDRA WICKRAMASEKARA, MARK SCANLON

19:00-21:00 GALA DINNER - FIESTA ROOM (COATES STUDENT CENTER)
09:00-10:30  SESSION 07 PRESENTATIONS (Chair: Dr. Milan Tuba)

**Dicke Hall 104 - Mabee Auditorium (In Person)**

**Paper ID 12:** Infeasibility of Sequitur-based Motif for Mouse Dynamics in Digital Forensics  
Richard Adeyemi Ikuesan, Farkhund Iqbal, Kadhim Hayawi

**Paper ID 39:** Smartphone Forensics: A Comparative Study of Common Mobile Phone Models  
Abduljalil Alblooshi, Naser Alineibi, Farkhund Iqbal, Richard Adeyemi Ikuesan, Zainab Khalid

**Paper ID 46:** Digital Forensics Analysis of YouTube, Instagram, and TikTok on Android Devices: A Comparative Study  
Chiamaka J Femi-Adeyinka, Nuri Kose, Tosin Akinsowon, Cihan Varol

**Paper ID 69:** Behind (Digital Crime) Scenes - An MSC Model  
Mario Raciti, Giampaolo Bella

**Paper ID 71:** Digital Forensic Methodology for Encryption Key Recovery from Black-Box IoT Devices  
Muhammad Rusyaidi Zunaidi, Asanka P Sayakkara, Mark Scanlon

**Paper ID 77:** Multimedia Forensics: Preserving Video Integrity with Blockchain  
Oluwasola Mary Adeyinka, Sahilkumar AHIR

**Paper ID 89:** Cybersecurity Data Visualization: Designing a Course for Future High School Students  
Shafi Parvez Mohammed, Syed Yaseen Quadri Ameen, Gahangir Hossain

**Paper ID 126:** The Development of a Digital Forensic Framework for Ease of Forensic Analysis  
Mahika Gupta, Dhruv Suvarna, Mahesh KM, Sonal Gabburi, Prasad B Honnavalli, Sapna V M

09:00-10:30  SESSION 08 PRESENTATIONS (Chair: Dr. Mark Lewis)

**Dicke Hall 108 (Online)**

**Paper ID 71:** A Digital Forensic Methodology for Encryption Key Recovery from Black-Box IoT Devices  
Muhammad Rusyaidi Zunaidi, Asanka P Sayakkara, Mark Scanlon

**Paper ID 77:** Multimedia Forensics: Preserving Video Integrity with Blockchain  
Oluwasola Mary Adeyinka, Sahilkumar AHIR

**Paper ID 89:** Cybersecurity Data Visualization: Designing a Course for Future High School Students  
Shafi Parvez Mohammed, Syed Yaseen Quadri Ameen, Gahangir Hossain

**Paper ID 94:** Demystifying knitr Package: Essential Recipes and Easy Steps for Adding Knit-Engines in R  
Sagiru Mati, Salim Jibrin Danbatta, Asaf Varol, Ahad Nasab, Abdullahi Garba Usman, Berna Uzun, Ahmad Nuhammad

**Paper ID 108:** Evaluation and Analysis of a Digital Forensic Readiness Framework for the IIoT  
Sri Harsha Mekala, Zubair Baig, Adnan Anwar, Naeem Firdous Syed

**Paper ID 126:** The Development of a Digital Forensic Framework for Ease of Forensic Analysis  
Mahika Gupta, Dhruv Suvarna, Mahesh KM, Sonal Gabburi, Prasad B Honnavalli, Sapna V M

10:30-10:45  Coffee Break
10:45-12:30  **SESSION 09 PRESENTATIONS** *(Chair: Dr. Paul Myers)*

**DICKE HALL 104 - MABEE AUDITORIUM (In Person)**

**Paper ID 25:**  Android Trojan Horse Spyware Attack: A Practical Implementation  
Collins Mbwiwa Mwange, Ebru Cankaya

**Paper ID 36:**  Why Phishing Emails Escape Detection: A Closer Look at the Failure Points  
Arifa Islam Champa, Md Fazle Rabbi, Minhaz Fahim Zibran

**Paper ID 41:**  The Trajectory of Romance Scams in the U.S.  
Ld Herrera, John Hastings

**Paper ID 48:**  Key Exchange with Diffie-Hellman Protocol and Composite Hash-Functions  
Manuel A Cardona-López, Juan Chimal-Egüía, Víctor Silva-García, Rolando Flores-Carapia

**Paper ID 73:**  LLM-Based Framework for Administrative Task Automation in Healthcare Environments  
Senay Gebreab, Khaled Salah, Raja Jayaraman, Muhammad Habib ur Rehman, Samer Ellahham

**Paper ID 104:**  Image-Based PDF Malware Detection Using Pre-Trained Deep Neural Networks  
Tyle Nichols, Jack Zemlanicky, Zhirui Luo, Qingqing Li, Jun Zheng

10:45-12:30  **SESSION 10 PRESENTATIONS** *(Chair: Dr. Eva Tuba)*

**DICKE HALL 108 (Online)**

**Paper ID 26:**  Generative Artificial Intelligence in Latin American Higher Education: A Systematic Literature Review  
Maria Baldeon Calisto, Alejandra De la Torre

**Paper ID 40:**  A Comparative Analysis of Vision Transformers and Convolutional Neural Networks in Cardiac Image Segmentation  
Maria Baldeon Calisto, Sebastian Granizo, Milena Iñiguez, Danny Navarrete, Daniel Riofrío, Noel Pérez-Pérez, Diego Benítez, Ricardo Flores-Moyano

**Paper ID 53:**  Comparison of Pre-Trained Models for Optimized Transformer Based Question Answering System  
Tunahan Gokcimen, Bihter Daş

**Paper ID 91:**  Enhanced UAV Security: Optimizing Accuracy and Efficiency with MSBCE Feature Selection  
Tomojit Ghosh, Shahnewaz Sakib

**Paper ID 105:**  Text Encryption Using Audio with Multiple Chaotic Maps  
Aayushman Singh, Kurunandan Jain

**Paper ID 115:**  A Comparison Between Transformers and Foundation Models in Sentiment Analysis of Student Evaluation of Teaching  
Inés Micaela Vega, José Valencia, Ángel Arcos, Danny Navarrete, Maria Baldeon Calisto

**Paper ID 150:**  Image Forgery Detection Using Convolutional Neural Networks  
Ayesh Buddhima Meepaganithage, Suman Rath, Mircea Nicolescu, Monica Nicolescu, Shamik Sengupta

**Paper ID 155:**  Feature Selection Using Pearson Correlation with Lasso Regression for Intrusion Detection System  
Iwan H Putro, Tohari Ahmad
12:30-14:00  **LUNCH AND CLOSING REMARKS (DICKE HALL JOHN AND JANICE BRAZIL COMMONS)**

14:00-15:30  **SESSION 11 PRESENTATIONS (CHAIR: DR. ASAFIG VAROL)**

**DICKE HALL 104 - MABEE AUDITORIUM (ONLINE)**

**PAPER ID 34:** ANDROPack: A Hybrid Method To Detect Packed Android Malware With Ensemble Learning  
Saranya Chandran, Mithun M

**PAPER ID 63:** Understanding Microbenchmark Detection of Existing Exploits in Apple M1 and M2 Chips  
Dr Richard Ward

**PAPER ID 118:** Multi-tenant Cloud Security Risk Prediction Through Cyber-Value-at-Risk (CVAR)  
Prashant Vajpayee

**PAPER ID 119:** Catch’em all: Classification of Rare, Prominent, and Novel Malware Families  
Maksim E Eren, Ryan Barron, Manish Bhattarai, Selma Wanna, Nicholas Solovyev, Kim Rasmussen, Boian Alexandrooe, Charles Nicholas

**PAPER ID 131:** Dynamic Calculation of Password Salts for Improved Resilience Towards Password Cracking Algorithms  
Oluwasola Mary Adedayo, Arun Mani

**PAPER ID 149:** Framework for Early Cyber Attack Detection Using ML Models Deployed On Fog Devices  
Uday Aditya Kasturi, Prateek N Kamath, Yuktha Poral, Baddela Divya Malika, Vadiraja Acharya

14:00-15:30  **SESSION 12 PRESENTATIONS (CHAIR: DR. TIMEA BEZDAN)**

**DICKE HALL 108 (ONLINE)**

**PAPER ID 28:** Handling Imbalanced Data for Detecting Scams in Ethereum Transactions Using Sampling Techniques  
Lakshmi Priya Krishnan, Iman Vakilinia, Sandeep Reddivari, Sanjay Ahuja

**PAPER ID 61:** Load Characterization of AI Applications Using DQoS Scheduler for Serving Multiple Requests  
Taufiq Odhi Dwiputra, Royyana Muslim Ithiadie, Tohari Ahmad

**PAPER ID 117:** The Reliability of Digital Evidence in Criminal Proceedings and the Potential Utilization of Artificial Intelligence in the Evidence Evaluation Process  
Sefa Ata, Çetin Arslan

**PAPER ID 123:** Assessing the Integrity of Mobile Platform-Based Sensor Data Pipelines  
Jordan Shropshire

**PAPER ID 142:** Using ITIL as part of the NIST Cybersecurity Framework  
Paulo S Teixeira, Sérgio Lopes, Sandro Carvalho, Patrícia Isabel Sousa Trindade da Leite

**PAPER ID 147:** Assessing the Health of a Network Under Attack  
Pedro Marques, Alfie Beard, Jonathan Francis Roscoe

XIV
14:00-15:30  WAPAIS & ISDFS PRESENTATIONS (CHAIR: DR. NUNO LOPEZ)

DICKE HALL 108 (ONLINE)

PAPER ID 18:  MACHINE LEARNING ASSISTED WEB APPLICATION FIREWALL
Pranav G Kalariya, Yasser Alginahi, Manthan Jethva

PAPER ID 55:  TOPIC MODELLING USING BERTOPIC FOR ROBUST SPAM DETECTION
Tunahan Gokcimen, Bihter Daş

PAPER ID 114:  MALWARE API CALL-BASED MULTICLASS-CLASSIFICATION USING MACHINE LEARNING AND DEEP LEARNING
Sarah Adair, Cihan Varol, Fan Liang, Van Vung Pham

PAPER ID 141:  AI BASED GOALKEEPER FOR PENALTY SHOT PREDICTION USING RNN AND PATTERN MATCHING ALGORITHM
Akshita Naithani, Vrishin Jain, Tanish Singh Rajpal, Vansh Mistry

PAPER ID 154:  EVOLUTIONARY ANALYSIS OF ADHERENCE TO THE ISO 27001:2013 STANDARD IN PORTUGAL: REGIONAL AND SECTORAL STUDY
Inês Alves, Paulo S Teixeira, Nuno Lopes

PAPER ID 171:  INVESTIGATION OF EFFICIENCY AND ACCURACY OF DEEP LEARNING MODELS AND FEATURES WITH ELECTROENCEPHALOGRAM (EEG) DATA FOR BINARY CLASSIFICATION
Kelly O'Brien, Liam Brown, Joaquim González

15:30-17:00  SESSION 13 PRESENTATIONS (CHAIR: TBD)

DICKE HALL 104 - MABEE AUDITORIUM (ONLINE)

PAPER ID 22:  PERSISTENT BROWSER STORAGE DATA EXTRACTOR
Fnu Aakanksha, Avinash Kumar, Cihan Varol, Hyuk Cho, Amar A Rasheed

PAPER ID 44:  EVALUATION OF DIFFERENT PASSIVE METHODS FOR LIVENESS DETECTION
Marius Butz, Matthias Wölfel

PAPER ID 62:  UNVEILING DIGITAL SECRETS: AN IMAGE TEXT VISION APP FOR ENHANCED DIGITAL FORENSICS INVESTIGATIONS
Supriya S Bandal, Suman Rath

PAPER ID 56:  MULTI-LABEL CLASSIFICATION IN TEXT DATA: AN EXAMINATION ON INNOVATIVE TECHNOLOGIES
Pınar Savcı, Bihter Daş

PAPER ID 116:  PERSISTENCE TECHNIQUES IN MICROSOFT ACTIVE DIRECTORY: DETECTION AND MITIGATION STRATEGIES
Zeyneb Senturk, Erdal Irmak

PAPER ID 152:  CYBER-SECURITY KNOWLEDGE GRAPH GENERATION BY HIERARCHICAL NONNEGATIVE MATRIX FACTORIZATION
Ryan C Barron, Maksim E Eren, Manish Bhattacharjya, Selma Wanna, Nicholas Solovyev, Kim Rasmussen, Boian Alexandrov, Charles Nicholas, Cynthia Matuszek
15:30-17:00 Session 14 Presentations (Chair: TBD)

Dicke Hall 108 (Online)

Paper ID 86: Evaluation of Privacy-Utility Tradeoff in Generative Adversarial Network Variants
Shahnewaz Karim Sakib, Tomojit Ghosh

Paper ID 110: Boosting Aircraft Monitoring and Security through Ground Surveillance Optimization with YOLOv9
Murat Bakirci, Irem Bayraktar

Paper ID 111: YOLOv9-Enabled Vehicle Detection for Urban Security and Forensics Applications
Murat Bakirci, Irem Bayraktar

Paper ID 129: ORAT - Open Redirect Analysis Tool
José Martinho, Diogo Mendes, Pedro Pinto

Paper ID 153: Occupancy Grid Map Completion Based on Geometric Features and Door Discovery
Selma Güzel, Erkan Uslu, Sirma Yavuz

Paper ID 166: A Real-Time Hand Sign Language Recognition System for Threatening Situations Using Deep Learning
Zardasht A. A. Shwany, Shayda Khudhur Ismaiel, Karwan Hoshyar Khalid, Twana Mustafa, Murat Karabatak

17:00-18:00 Session 15 Presentations (Chair: Dr. Eva Tuba)

Dicke Hall 104 - Mabee Auditorium (Online)

Paper ID 15: A Study of Fine-Tuned Language Models in Vulnerability Classification
Onyeka Ezenwoye, Eduard C Pinconschi

Paper ID 37: A Comprehensive Spectrum of Open Ports
Rashad Aliyev

Paper ID 54: Structured Named Entity Recognition (NER) in Biomedical Texts Using Pre-Trained Language Models
Pinar Savcı, Bihter Daş

Paper ID 58: AbuseGPT: Abuse of Generative AI ChatBots to Create Smishing Campaigns
Ashfak Mo Shibu, Mir Mehedi A Pritom, Maanak Gupta

Paper ID 148: Towards Next-Generation Smart Sandboxes: Comprehensive Approach to Mobile Application Security
Ezgi Güçüyener, Mehmet Amaç Güvensan

Hafzullah İş
17:00-18:00  **SESSION 16 PRESENTATIONS (Chair: Dr. Milan Tuba)**

**DICKE HALL 108 (ONLINE)**

**PAPER ID 38:**  Few-Shot Multi-Label Multi-Class Classification with CLIP Model: Empowering Labels
Yagmur Aktas, Jorge García

**PAPER ID 51:**  Investigating Social Media Interactions on Edge and Chrome Browsers
Jeffrey D Berg, Kubra Gundogan, Cihan Varol

**PAPER ID 59:**  Deleted File Recovery for the Linux File System (Ext4): Finding the State-of-the-Art
Sai Bharadwaj Sirivaram, Sankadas Roy

**PAPER ID 97:**  A Review of Advancements and Applications of Pre-trained Language Models in Cybersecurity
Zefang Liu

**PAPER ID 107:**  Cognitive Modelling of Bankruptcy Risk: A Comparative Analysis of Machine Learning Models to Predict the Bankruptcy
Mahadi Hasan, Musfika Jannat Mamata, Jahirul Islam, Sabuj Saha, Ali Mahmud

**PAPER ID 130:**  Efficient Programmable Architecture for LWC NIST FIPS Standard ASCON
Islam A Elsadek, Islam Tawfiq

**PAPER ID 156:**  Cloud Cost Factors and AWS Cost Optimization Techniques
Ganesh Kumar Murugesan

---

**SESSION 17 Off-Line Video Presentations (Click to access the presentations)**

**PAPER ID 3:**  Ensemble Learning Model for Face Swap Detection
Khoulood Samrout, Nicolas Beluve, Olivier Deforges, Nader Bakir, Wassim Hamidouche

**PAPER ID 5:**  Research on Network Security Measurement on the Basis of Defense-in-Depth
Kunpeng Cao, Leyi Zhang

**PAPER ID 13:**  Classify Attacks Based on Blockchain Components
Anandhu S, Narayanan Subramanian

**PAPER ID 16:**  Guarding Voices, Protecting Homes: A Comprehensive Case Study on Voice Assistant Security in Smart Living
Fazal Ur Rehman Hashmi

**PAPER ID 21:**  iOS Mobile Forensics Methodologies, Extracting Biome Artifacts, and Overlooked Artifacts Needed to Improve Investigations
Mario Merendon, Cihan Varol, Narasimha K Shashidhar, Kirk Burns

**PAPER ID 45:**  Adversarial Cross-laser Attack: Effective Attack to DNNs in the Real World
Hanyu Wu, Ke Yan, Peng Xu, Bei Hui, Ling Tian

**PAPER ID 47:**  Mobile Forensic Investigation: Extractions and Connectivity Isolation in Phones Utilizing eSIM, ISIM Technology
Nurettin S Senol, Amar A Rasheed, Narasimha Karpoor Shashidhar

**PAPER ID 60:**  Forensic Analysis of an IoT ARP Spoofing Attack
Sabrina Friedl, Günther Pernul
PAPER ID 70:  **Securing Artificial Intelligence: Exploring Attack Scenarios and Defense Strategies**  
İrem Zehra Altun, Abdurrahman Emre Ozkok

PAPER ID 113:  **Enhancing Forensic Analysis with Autonomous UAV Deployment for Aerial Investigation**  
Murat Bakirci, Muhammed Miraç Özer

PAPER ID 127:  **ForTT-Gen: Network Traffic Generator for Malware Forensics Analysis Training**  
Jonas V Bistene

PAPER ID 128:  **Anti-forensics Under Scrutiny: Assessing the Effectiveness of Digital Obfuscation in the Cloud**  
Christopher Lowetz, Grant Shepard, Joel Coffman

PAPER ID 133:  **Privacy-Enhanced Image Restoration in Remote Sensing via Federated Learning**  
Muhammad Jahanzeb Khan, Suman Rath, Muhammad Hassan Zaib

PAPER ID 144:  **Investigation of Pre-service Teachers’ Digital Well-Being Levels with Respect to Various Variables**  
Ebū Polat, Songül Karabatak, Müslim Alanoğlu

PAPER ID 146:  **Investigation of Teachers’ Knowledge Management and Knowledge Hiding Behaviors**  
Songül Karabatak, Müslim Alanoğlu, Ebū Polat

PAPER ID 164:  **Advancements in Object Detection For Unmanned Aerial Vehicles: Applications, Challenges, and Future Perspectives**  
Anıl Sezgin, Aytuğ Boyacı

PAPER ID 165:  **Deep Learning Based Brain Tumor Classification for MR Images using ResNet50**  
Ömer Miraç Kökçam, Aytuğ Boyacı, Muhammed E Çolak

PAPER ID 168:  **Examination of Object Tracking Studies Using Deep Learning: A Bibliometric Analysis Study**  
Sevinç Ay, Songül Karabatak, Murat Karabatak

PAPER ID 169:  **Bibliometric Analysis of Artificial Intelligence in Utilized Distance Education and Distance Learning Studies**  
Sevinç Ay, Songül Karabatak, Murat Karabatak

PAPER ID 172:  **Examining the Relationship between Digital Well-Being, Digital Hoarding and Mobile Information Security Awareness with Association Rule**  
Songül Karabatak, Müslim Alanoğlu, Murat Karabatak

PAPER ID 173:  **Comparison of IDS in IoT, Mobile and Cloud Based Systems**  
Görkem Gök, Aytuğ Boyacı, Mustafa Ulas

PAPER ID 174:  **Classification of ECG Signals Encrypted with CNN Based Autoencoder with LSTM**  
Merve Akkuş, Murat Karabatak, Ramazan Tekin

PAPER ID 175:  **Investigation of Teacher Candidates’ Digital Obesity**  
Sevinç Ay, Songül Karabatak, Murat Karabatak

PAPER ID 176:  **Discovery of New Chaotic Systems: Based on Existing Systems**  
Tuncay Cigal, Erkan Tanyıldızı
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensemble Learning Model for Face Swap Detection</td>
<td>1</td>
</tr>
<tr>
<td>Research on Network Security Measurement on the Basis of Defense-In-Depth</td>
<td>1</td>
</tr>
<tr>
<td>SDN Security Channel Constructed Using SM9</td>
<td>1</td>
</tr>
<tr>
<td>Analyzing Cryptocurrency Social Media for Price Forecasting and Scam Detection</td>
<td>2</td>
</tr>
<tr>
<td>Infeasibility of Sequitur-based Motif for Mouse Dynamics in Digital Forensics</td>
<td>2</td>
</tr>
<tr>
<td>Classify Attacks Based on Blockchain Components</td>
<td>2</td>
</tr>
<tr>
<td>A Study of Fine-Tuned Language Models in Vulnerability Classification</td>
<td>3</td>
</tr>
<tr>
<td>Guarding Voices, Protecting Homes: A Comprehensive Case Study on Voice Assistant Security in Smart Living</td>
<td>3</td>
</tr>
<tr>
<td>Machine Learning Assisted Web Application Firewall</td>
<td>3</td>
</tr>
<tr>
<td>Adversarial Machine Learning for Detecting Advanced Threats Inspired by StuxNet in Critical Infrastructure Networks</td>
<td>4</td>
</tr>
<tr>
<td>IOS Mobile Forensics Methodologies, Extracting Biome Artifacts, and Overlooked Artifacts Needed to Improve Investigations</td>
<td>4</td>
</tr>
<tr>
<td>Persistent Browser Storage Data Extractor</td>
<td>4</td>
</tr>
<tr>
<td>Performance Comparison Analysis of Digital Forensic Tools in Various Operating Systems</td>
<td>5</td>
</tr>
<tr>
<td>Android Trojan Horse Spyware Attack: A Practical Implementation</td>
<td>5</td>
</tr>
<tr>
<td>Generative artificial intelligence in Latin American higher education: a systematic literature review</td>
<td>6</td>
</tr>
<tr>
<td>Handling Imbalanced Data for Detecting Scams in Ethereum Transactions using Sampling Techniques</td>
<td>6</td>
</tr>
<tr>
<td>Chaos-Based Stream Ciphers for 5G Inter-slice Network Security</td>
<td>6</td>
</tr>
<tr>
<td>Comparative Analysis of Automated Scanning and Manual Penetration Testing for Enhanced Cybersecurity</td>
<td>7</td>
</tr>
<tr>
<td>AndroPack: A Hybrid Method to Detect Packed Android Malware With Ensemble Learning</td>
<td>7</td>
</tr>
<tr>
<td>Analyzing Insider Cyber Threats and Human Factors within the Framework of Agriculture 5.0..</td>
<td>7</td>
</tr>
<tr>
<td>Why Phishing Emails Escape Detection: A Closer Look at the Failure Points</td>
<td>8</td>
</tr>
<tr>
<td>A Comprehensive Spectrum of Open Ports</td>
<td>8</td>
</tr>
<tr>
<td>Few-Shot Multi-Label Multi-Class Classification for Dark Web Image Categorization</td>
<td>8</td>
</tr>
<tr>
<td>Smartphone Forensics: A Comparative Study of Common Mobile Phone Models</td>
<td>9</td>
</tr>
<tr>
<td>A Comparative Analysis of Vision Transformers And Convolutional Neural Networks in Cardiac Image Segmentation</td>
<td>9</td>
</tr>
</tbody>
</table>
The Trajectory of Romance Scams in the U.S. ................................................................. 9
Opinions Evolution Analysis in Time-varying Social Networks: A Silent Spiral Opinion Model .. 10
Evaluation of Different Passive Methods for Liveness Detection .................................. 10
Adversarial Cross-laser Attack: Effective Attack to DNNs in the Real World .................. 10
Digital Forensics Analysis of YouTube, Instagram, and TikTok on Android Devices: A Comparative Study ........................................................................................................... 11
Mobile Forensic Investigation: Extractions and Connectivity Isolation in Phones Utilizing eSIM, iSIM Technology ........................................................................................................... 11
Key Exchange with Diffie-Hellman Protocol and Composite Hash-Function .................... 11
Identifying Social Media Interactions on Edge and Chrome Browsers ............................... 12
Identifying Malware Family with String Matching Algorithms Based on API Calls and Entire Strings ......................................................... 12
Comparison of Pre-trained Models for Optimized Transformer Based Question Answering System .............................................................................................................................................. 13
Structured Named Entity Recognition (NER) in Biomedical Texts Using Pre-Trained Language Models .................................................................................................................................................. 13
Topic Modelling using BERTopic for Robust Spam Detection ........................................ 13
Multi-Label Classification in Text Data: An Examination on Innovative Technologies .......... 14
AbuseGPT: Abuse of Generative AI ChatBots to Create Smishing Campaigns ................ 14
Deleted file recovery for the Linux File System (Ext4): Finding the state-of-the-art .......... 14
Forensic Analysis of an IoT ARP Spoofing Attack ............................................................... 15
Load Characterization of AI Applications using DQoES Scheduler for Serving Multiple Requests ......................................................................................................................................................... 15
Understanding Microbenchmark Detection of Existing Exploits in Apple M1 and M2 Chips ..... 16
Exploring Security, Privacy, and Forensics Concerns in the Metaverse .............................. 16
Behind (Digital Crime) Scenes - An MSC Model ................................................................. 17
Securing Artificial Intelligence: Exploring Attack Scenarios and Defense Strategies ................ 17
A Digital Forensic Methodology for Encryption Key Recovery from Black-Box IoT Devices .... 17
Forensic Analysis of WhatsApp, Instagram, and Telegram on Virtual Android Device ........ 18
LLM-Based Framework for Administrative Task Automation in Healthcare ...................... 18
Recovery CAT: A Digital Forensics Tool for Cryptocurrency Investigations ..................... 18
A Robust Misbehavior Detection System for Cooperative Driving Network .................... 19
Multimedia Forensics: Preserving Video Integrity with Blockchain ................................... 19
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unraveling IoT Traffic Patterns: Leveraging Principal Component Analysis for Network Anomaly Detection and Optimization</td>
<td>19</td>
</tr>
<tr>
<td>Securing Healthcare 5.0: Exploring BYOD Cyber Risks, Misuse Cases, and Best Practices</td>
<td>20</td>
</tr>
<tr>
<td>Stream Clustering on A Forensic Timeline</td>
<td>20</td>
</tr>
<tr>
<td>Evaluation of Privacy-Utility Tradeoff in Generative Adversarial Network Variants</td>
<td>20</td>
</tr>
<tr>
<td>Security and Privacy Threats Posed by IoT Devices Used by Students on College Campuses</td>
<td>21</td>
</tr>
<tr>
<td>HNMblock: Blockchain Technology Powered Healthcare Network Model for Epidemiological Monitoring, Medical Systems Security, and Wellness</td>
<td>21</td>
</tr>
<tr>
<td>Cybersecurity Data Visualization: Designing a Course for Future High School Students Shafi Parvez</td>
<td>22</td>
</tr>
<tr>
<td>Enhanced UAV Security: Optimizing Accuracy and Efficiency with MSBCE Feature Selection</td>
<td>22</td>
</tr>
<tr>
<td>Econometric and AI-Based Modelling of Nigeria’s Interest Rates Based on Fisher Equation</td>
<td>22</td>
</tr>
<tr>
<td>Demystifying Knitr Package: Essential Recipes and Easy Steps for Adding Knit-Engines in R</td>
<td>23</td>
</tr>
<tr>
<td>A Review of Advancements and Applications of Pre-trained Language Models in Cybersecurity</td>
<td>23</td>
</tr>
<tr>
<td>DNS Tunnel Problem In Cybersecurity</td>
<td>23</td>
</tr>
<tr>
<td>Cyber Ready Rural: Understanding Law Enforcement Cyber Readiness</td>
<td>24</td>
</tr>
<tr>
<td>Image-based PDF Malware Detection Using Pre-trained Deep Neural Networks</td>
<td>24</td>
</tr>
<tr>
<td>Text Encryption Using Audio with Multiple Chaotic Maps</td>
<td>24</td>
</tr>
<tr>
<td>Examination of Artificial Intelligence Integration and Its Impact in Higher Education</td>
<td>25</td>
</tr>
<tr>
<td>Cognitive Modelling of Bankruptcy Risk: A Comparative Analysis of Machine Learning Models to Predict the Bankruptcy</td>
<td>25</td>
</tr>
<tr>
<td>Evaluation and Analysis of a Digital Forensic Readiness Framework for the IIoT</td>
<td>25</td>
</tr>
<tr>
<td>A Framework for Integrated Digital Forensic Investigation Employing AutoGen AI Agents</td>
<td>26</td>
</tr>
<tr>
<td>Boosting Aircraft Monitoring and Security through Ground Surveillance Optimization with YOLOv9</td>
<td>26</td>
</tr>
<tr>
<td>YOLOv9-Enabled Vehicle Detection for Urban Security and Forensics Applications</td>
<td>26</td>
</tr>
<tr>
<td>Enhancing Forensic Analysis with Autonomous UAV Deployment for Aerial Investigation</td>
<td>27</td>
</tr>
<tr>
<td>Malware API Call-Based Multiclass-Classification Using Machine Learning and Deep Learning</td>
<td>27</td>
</tr>
<tr>
<td>A Comparison Between Transformers and Foundation Models in Sentiment Analysis of Student Evaluation of Teaching</td>
<td>28</td>
</tr>
<tr>
<td>Persistence Techniques in Microsoft Active Directory: Detection and Mitigation Strategies</td>
<td>28</td>
</tr>
<tr>
<td>Multi-tenant Cloud Security Risk Prediction through Cyber-Value-at-Risk (CVaR)</td>
<td>29</td>
</tr>
<tr>
<td>Catch’em all: Classification of Rare, Prominent, and Novel Malware Families</td>
<td>29</td>
</tr>
</tbody>
</table>
Effect of Signal Conditioning and Evoked Potential based Representation on Stability and Distinctiveness of EEG Brain Signatures ................................................................. 29
Assessing the Integrity of Mobile Platform-Based Sensor Data Pipelines ......................... 30
The Development of a Digital Forensic Framework for Ease of Forensic Analysis ............ 30
ForTT-Gen: Network Traffic Generator for Malware Forensics Analysis Training .............. 30
Anti-forensics Under Scrutiny: Assessing the Effectiveness of Digital Obfuscation in ........... 31
ORAT - An Open Redirect Analysis Tool ............................................................................. 31
Efficient Programable Architecture for LWC NIST FIPS Standard ASCON ........................ 32
Dynamic Calculation of Password Salts for Improved Resilience Towards Password Cracking Algorithms ........................................................................................................... 32
Decoding DOOH Viewability Using YOLO for Privacy-Friendly Human Silhouette Identification on LiDAR Point Clouds .................................................................................... 32
Privacy-Enhanced Image Restoration in Remote Sensing via Federated Learning ............... 33
Towards Privacy-preserving Vehicle Digital Forensics: A Blockchain Approach ............... 33
Contribution of Algorithm Visualizations to Students’ Learning Skills: A Pedagogical Approach33
algoxSSF: Detection and analysis of cross-site request forgery (XSRF) and cross-site scripting (XSS) attacks via Machine learning algorithms .............................................................................. 34
AI Based Goalkeeper for Penalty Shot Prediction Using RNN and Pattern Matching Algorithm 34
Using ITIL as part of the NIST Cybersecurity Framework ..................................................... 35
Investigation of Pre-service Teachers’ Digital Well-Being Levels with Respect to Various Variables .................................................................................................................... 35
Investigation of Teachers’ Knowledge Management and Knowledge Hiding Behaviors ...... 35
Assessing the Health of a Network Under Attack .................................................................. 36
Towards Next-Generation Smart Sandboxes: Comprehensive Approach to Mobile Application Security ................................................................. 36
Image Forgery Detection Using Convolutional Neural Networks ......................................... 37
Cyber-Security Knowledge Graph Generation by Hierarchical Nonnegative Matrix Factorization ......................................................................................................................... 37
Occupancy Grid Map Completion Based on Geometric Features and Door Discovery ........ 38
Evolutionary analysis of adherence to the ISO 27001:2013 standard in Portugal: Regional and Sectoral Study .............................................................. 38
Feature Selection using Pearson Correlation with Lasso Regression for Intrusion Detection System ......................................................................................................................... 38
Cloud Cost Factors and AWS Cost Optimization Techniques ................................................ 39
Cassava Plant Disease Detection using Transfer Learning with Convolutional Neural Networks ......................................................................................................................... 39
Credible Diffusion: Improving Diffusion Models Interpretability with Transformer Embeddings
.................................................................................................................................39

Optimizing Machine Learning for Breast Cancer Detection by Hybrid Metaheuristic Approach
........................................................................................................................................40

LLM-Driven SAT Impact on Phishing Defense: A Cross-Sectional Analysis
........................................................................................................................................40

Advancements in Object Detection for Unmanned Aerial Vehicles: Applications, Challenges,
and Future Perspectives........................................................................................................40

Deep Learning Based Brain Tumor Classification for MR images using ResNet50
........................................................................................................................................41

A Real-Time Hand Sign Language Recognition System for Threatening Situations Using Deep
Learning....................................................................................................................................41

Examination of Object Tracking Studies Using Deep Learning: A Bibliometric Analysis Study...
........................................................................................................................................42

Bibliometric Analysis of Artificial Intelligence in Utilized Distance Education and Distance
Learning Studies........................................................................................................................42

Investigation of Efficiency and Accuracy of Deep Learning Models and Features with
Electroencephalogram (EEG) Data for Binary Classification...................................................42

Examining the Relationship between Digital Well-Being, Digital Hoarding and Mobile
Information Security Awareness with Association Rule ..........................................................43

Comparison of IDS in IoT, Mobile and Cloud Based Systems..................................................43

Classification of ECG Signals Encrypted with CNN Based Autoencoder with LSTM...............43

Investigation of Teacher Candidates' Digital Obesity ..............................................................44

Discovery of New Chaotic Systems: Based on Existing Systems .............................................44
ABSTRACTS

Paper ID 3

ENSEMBLE LEARNING MODEL FOR FACE SWAP DETECTION

Khouloud Samrouch (Arab Open University)*; Nicolas BEUVE (INSA Rennes); Olivier Deforges (IETR, Rennes); Nader Bakir (Beirut Arab University); Wassim Hamidouche (INSA Rennes)

*ksamrouch@aou.edu.lb

Deepfake videos become now one of the top research topics because of their high spreading rate on social media. Faceswap, a particular type of Deepfake, consists in swapping faces of two persons in a video. Hence, face swapping can have malicious uses, such as falsifying privacy, interfering with political campaigns, terrorism, and threatening the social stability of the countries. Thus, early detection of this fake content is a primary task to limit their spread.

Multiple approaches for DeepFake detection exist in the literature. The most recent and best ones are Identity-Aware and Mesoscopic features-based approaches. However, each of these approaches presents particular limitations.

Therefore, in this paper, we propose to take the best out of these two recent approaches and to optimize the performance and robustness of Deepfake content detection. In particular, we propose an Ensemble Learning model based on combining the best two methods from the two aforementioned most recent approaches of detection.

Our experiments show that our proposed ensemble model improved the performance and robustness of Deepfake detection to reach an accuracy of 95%.

---

Paper ID 5

RESEARCH ON NETWORK SECURITY MEASUREMENT ON THE BASIS OF DEFENSE-IN-DEPTH

Kunpeng Cao (ZTE Corporation)*; Leyi Zhang (ZTE corporation)

*cao.kunpeng1@zte.com.cn

With the widespread use of advanced network technologies such as cloud computing and AI, network environments become increasingly complicated, and network attacks also vary greatly. Then, how to exactly measure network security and take proactive measures in a timely manner to mitigate network attacks is of great importance for most network operators. This paper not only innovatively proposes a sophisticated network security measurement model based on NIST CSF philosophy, but also practices this model in a sample live network to prove its effectiveness, specifying a new way for in-depth network security measurement research.

---

Paper ID 10

SDN SECURITY CHANNEL CONSTRUCTED USING SM9

Dan Wang (Nuclear Power Institute of China)*; Liangyu Dong (China Industrial Control Systems Cyber Emergency Response Team); Tang Hua (Nuclear Power Institute of China); Junjie Gu (Nuclear Power Institute of China); Ziwei Liu (Nuclear Power Institute of China); Xintong You (Nuclear Power Institute of China)

wangdan9101@163.com

In relation to the utilization of SDN within the production environment, the process of constructing a secure flow table transmitting channel has elicited concerns from operations and maintenance personnel and researchers. Despite the fact that research findings can satisfy the security communication requirements of controllers and switches, they typically require escalated investment or operation and maintenance expenses, thereby making its implementation challenging. Aiming to rectify this, we have devised a streamlined secure channel construction methodology, employing the SDN device ID and timestamp as identity tags, and designing an identity authentication and password negotiation approach founded on these identity tags. Conclusively, the security evaluation of this methodology verifies that our method presents robust security in EUF-CMA.
Paper ID 11

ANALYZING CRYPTOCURRENCY SOCIAL MEDIA FOR PRICE FORECASTING AND SCAM DETECTION
Lakshmi Priya Krishnan (UNF); Iman Vakilinia (University of North Florida)*; Sandeep Reddivari (University of North Florida); Sanjay Ahuja (UNF)
i.vakilinia@unf.edu

The exponential growth of cryptocurrencies in the last decade has been accompanied by a surge in illicit activities, such as pump-and-dump schemes, Ponzi schemes, and exit scams. These nefarious activities have proliferated through the manipulation of social media platforms. This work employs a multi-modal approach to predict cryptocurrency price movements by analyzing social media data, search interest, tweet spikes, and historical cryptocurrency prices. Using data from social media discussions, we extract lexical and behavioral features that highlight sentiment shifts, influence tactics, and cross-platform correlations relevant to cryptocurrency price fluctuations. Using a Variational Autoencoder, this approach predicts cryptocurrency prices and unveils patterns of pump-and-dump attempts. With real-time deployment capabilities, this system not only aids investors in understanding and predicting price trends but also offers protection against scams that may coincide with unusual price fluctuations. Moreover, the techniques developed extend to detecting manipulation and organized inauthenticity beyond the realm of cryptocurrency, ensuring trust and security in digital systems.

Paper ID 12

INFEASIBILITY OF SEQUITUR-BASED MOTIF FOR MOUSE DYNAMICS IN DIGITAL FORENSICS
Richard Adeyemi Ikuesan (Zayed University)*; Farkhund Iqbal (Professor, Zayed University); Kadhim Hayawi (Zayed University)
richard.ikuesan@zu.ac.ae

Utilizing and deploying behavioral biometric modalities (BBM), specifically mouse dynamics for user attribution in a digital investigation, has seen a rapid upsurge. However, as asserted in a recent study, the current reliability threshold of BBM falls short of the required standard for forensic attributes. This poor reliability can be attributed, in part, to the low signal-to-noise ratio in a typical behavioral dataset. This study proposed a context-free signature identification and extraction technique for BBM to extract a unique mouse dynamics signature suitable for a forensic process. A Re-Pair Grammar induction approach, which identifies and extracts unique Grammar sequences, was used to achieve this proposition. The grammar generation leverages symbolic aggregate approximation techniques to generate behavioral string subsequences from the mouse dataset. The Re-Pair approach was then used to develop a user attribution mechanism, which can be deployed for digital forensic analysis. The outcome of the implementation of the proposition, however, shows a poor performance relative to existing studies, hence its infeasibility as a benchmark for forensic science. However, it shows promising potential to reveal the inherent noise in mouse dynamics data, which can provide further insight into digital forensic science. This result further extends the literature on establishing digital forensic science, a significant requirement for any forensic discipline.

Paper ID 13

CLASSIFY ATTACKS BASED ON BLOCKCHAIN COMPONENTS
Anandhu S (Amrita Vishwa Vidyapeetham)*; Narayanan Subramanian (Amrita Vishwa Vidyapeetham)
anandhuds2231@gmail.com

Blockchain technology has become a ground-breaking instrument for guaranteeing data integrity, protecting digital transactions, and facilitating decentralized consensus across a range of applications. On the other hand, a number of cyberattacks pose a threat to its unbreakable exterior and widespread acceptance. In order to comprehend and describe the security issues that these essential blockchain components may encounter, we examine potential vulnerabilities in them in this review paper. We concentrate our analysis on the mining operations that are the foundation of cryptocurrency production, the consensus mechanisms that support the integrity of blockchains, and the mining pools that raise concerns about centralization in a decentralized system. We also examine the peer-to-peer network structure, which is a strength and a weakness, the immutable ledger system, the digital wallets that store cryptographic currencies, and the underlying network that functions as the backbone of the blockchain. Special consideration is given to smart
contracts, which have proven to be vulnerable to flaws that astute attackers can take advantage of, despite their objective and automated execution design. Our objective is to provide a thorough analysis of the security issues and attack vectors present in blockchain components by looking into these areas. We also hope to provide insights into the actions required to strengthen these systems against possible threats. For researchers, developers, and consumers who believe that technology will offer a safe, untrusted foundation for upcoming advancements in the fintech and cryptocurrency industries, this investigation is essential.

Paper ID 15
A STUDY OF FINE-TUNED LANGUAGE MODELS IN VULNERABILITY CLASSIFICATION
Onyeka Ezenwoye (Augusta University)*; Eduard C Pinconschi (Universidade do Porto)
ocezenwoye@augusta.edu
This empirical study looks at fine-tuning four OpenAI pre-trained models to classify vulnerability data by software type. Leveraging a labeled dataset, the efficacy of the models is explored. The research question addresses the effectiveness of fine-tuned pre-trained models as classifiers. Through a series of experiments, models' performance and influencing factors are identified. The research design, fine-tuning methodology, and evaluation results are described. This work shows the models attain remarkable accuracy. It contributes valuable insights to the application of pre-trained language models in enhancing software vulnerability classification for improved software security.

It contributes valuable insights to the application of pre-trained language models in enhancing software vulnerability classification for improved software security.

Paper ID 16
GUARDING VOICES, PROTECTING HOMES: A COMPREHENSIVE CASE STUDY ON VOICE ASSISTANT SECURITY IN SMART LIVING
Fazal Ur Rehman Hashmi (National University of Sciences and Technology)*; Joudat Hashmi (Georgia Tech University); Moiz Abdullah (Air University Islamabad); Hafsah Zaman (National University of Sciences and Technology)
fhashmi.msis23seecs@seecs.edu.pk
The evolution of technologies in the last decades has transformed the whole human interaction experience with the digital world. Integrated into users’ home voice assistant devices has rationalized personal interaction with the technology however convenience of intelligent voice assistant presents security and privacy risks. This paper investigates the security vulnerabilities of smart voice assistant devices specifically focusing on Google Home Mini. Through a series of simulated attacks and comprehensive analysis, this study uncovers potential risks ranging from unauthorized access to user data privacy compromise within home networks. The objective is to raise awareness about these vulnerabilities and their implication urging the need for robust security measures and providing valuable observation for future research. As voice devices are becoming an integral part of daily life addressing these challenges is paramount to ensuring user privacy data integrity and overall security of the smart home ecosystem.

Paper ID 18
MACHINE LEARNING ASSISTED WEB APPLICATION FIREWALL
Pranav G Kalariya (University of windsor)*; Yasser Alginahi (University of Windsor); Manthan Jethva (University of Windsor)
kalarya@uwindsor.ca
This project presents the development and implementation of a sophisticated Web Application Firewall (WAF) empowered by machine learning techniques to bolster cybersecurity measures. Traditional WAFs primarily rely on rule-based systems, which may struggle to adapt to the evolving nature of web-based threats. In contrast, our proposed solution leverages machine learning algorithms to dynamically analyze and respond to emerging cyber threats, providing a more proactive and adaptive defense mechanism. The core functionality of the system involves the continuous monitoring of incoming web traffic, extracting relevant features, and utilizing a machine learning model to
classify the traffic as either benign or malicious. The model is trained on historical data to recognize patterns and behaviors indicative of various cyber threats, including SQL injection, cross-site scripting, and other common attack vectors. Through this learning process, the system becomes adept at discerning malicious activities and adapting its defense strategies accordingly. The proposed model helps achieve higher precision in identifying the threat requests from normal requests.

Paper ID 20

ADVERSARIAL MACHINE LEARNING FOR DETECTING ADVANCED THREATS INSPIRED BY STUXNET IN CRITICAL INFRASTRUCTURE NETWORKS

Hafiz Bilal Ahmad (Xidian University)*, HaiChang Gao, NaiLa Latif, Abdul Aziiz, Muhammad Auraangzeb, and Muhammad Tanveer Khan

engr.hbahmad@gmail.com

Inspired by the notorious StuxNet malware, this paper presents a unique and resilient architecture to address the imminent issue of identifying advanced threats within critical infrastructure networks. We use adversarial machine learning techniques to keep ahead of ever-changing threats. Our defense system's fundamental component is a Multi-Layer Perceptron (MLP) architecture that we've dubbed "StuxNet." This innovative method combines threat intelligence, anomaly detection, and deep learning to forecast and counter sophisticated attacks. The effectiveness of our method in bolstering the security of critical infrastructure networks is supported by empirical evaluations and real-world case studies. Importantly, the StuxNet-MLP architecture has a 98 percent detection accuracy for sophisticated threats. These results highlight the paramount significance of preventative cybersecurity measures in protecting mission-critical systems and provide useful insights for fending off sophisticated attacks. To ensure a safer and more resilient digital future, this study highlights the need to stay ahead in the continuous battle to secure key infrastructure.

Paper ID 21

IOS MOBILE FORENSICS METHODOLOGIES, EXTRACTING BIOME ARTIFACTS, AND OVERLOOKED ARTIFACTS NEEDED TO IMPROVE INVESTIGATIONS

Mario Merendon (Sam Houston State University); Cihan Varol (Sam Houston State University)*; Narasimha K Shashidhar (SHSU); Kirk Burns (Sam Houston State University)
cvarol@shsu.edu

Digital forensic examiners are guided by best practices and methodologies to ensure their examinations and findings are sound and can hold up in a court of law. Apple iPhones are among the top two producing mobile devices on the market and account for a large portion of examinations by law enforcement and defense experts. Similarly, the data iOS devices have the ability to store and their evidentiary value are more important than ever as prosecution and defense rely on examiner findings that have far reaching consequences for those on trial. This paper will explore the options available for many iOS devices and the difference in data that can be obtained between Advance Logical and Full File System extractions. Additionally, it will describe some high-level artifacts and provide some best practices for the examiner to consider in order to get the most out of the examination and most importantly, obtain a full-picture and context of what courts rely on, facts and the truth.

Paper ID 22

PERSISTENT BROWSER STORAGE DATA EXTRACTOR

Fnu Aakanksha (Sam Houston State University); Avinash Kumar (Sam Houston State University); Cihan Varol (Sam Houston State University)*; Hyuk Cho (Sam Houston State University); Amar A Rasheed (Sam Houston State University)
cvarol@shsu.edu

With the recent development in the World Wide Web, browsers have become more sophisticated, and they can store data locally to provide a faster and user-friendly browsing experience. The locally stored data can be the treasure of information for the digital investigators because using this information can help in solving a crime by discovering any
suspect-related information. Browsers can store data in various storage areas such as History, Local Storage, IndexedDB, Cookies, etc. As a digital forensic investigator, it can become tedious to go to every storage mechanism and look for the stored information for a particular website visit. Therefore, this research is going to provide a mechanism, a Proof of Concept user-friendly GUI-based application, where digital investigators can extract all related data about a particular website visit. This work will incorporate three different browsers, Google Chrome, Opera, and Mozilla Firefox. Not only showing the aggregated view of the extracted data, but digital investigators will also have an option to search data by using a specific domain or event and get all the information related to that domain or event in a unified format.

**Paper ID 24**

**PERFORMANCE COMPARISON ANALYSIS OF DIGITAL FORENSIC TOOLS IN VARIOUS OPERATING SYSTEMS**

Athanasios Manios (IEEE member)*; Christos Liambas (University of East London/Metropolitan College/Aristotle University of Thessaloniki)

manios.ath@gmail.com

It is known that experts widely use digital forensics tools, in order to investigate criminal cases. The main scope of this research is considered as the performance comparison of digital forensic tools in various Operating Systems, such as “Windows 10”, “Windows 11”, “Ubuntu”, and “Windowsfx”. This is done for optimization reasons and more specifically for the minimization of processing time in forensic data analysis. The research was divided into two main parts by using exactly the same hardware as well as the default Operating Systems' configuration. The first part presents the performance comparison of the above Operating Systems by using two benchmarking tools such as “Phoronix Test Suite” and “Indigobench”. The second part focuses on the performance measurements of the corresponding digital forensic tools “FTK Imager”, “Photorec”, “Quickhash” and “Peautils”. It should be noted that every tool is tested ten times in order to increase the accuracy of the averaged total execution time of every iteration. The results indicate that the “Windowsfx” Operating System has the best overall performance after exhausting research of testing all the aforementioned tools.

**Paper ID 25**

**ANDROID TROJAN HORSE SPYWARE ATTACK: A PRACTICAL IMPLEMENTATION**

Collins Mbwika Mwange (University of Texas at Dallas); Ebru Cankaya (University of Texas at Dallas)*

exc067000@utdallas.edu

Considering the popularity of rapidly growing mobile device use, this study delves into the persistent threat of Trojan horses, focusing on one select mobile OS platform, Android. To demonstrate the heightened risk Trojan horses pose due to their seemingly benign nature, we develop a novel deliberate Trojan horse spyware from scratch to discreetly harvest sensitive data from Android devices. This spyware can clandestinely access device information such as SMSs, contacts, call logs, and installed apps, transmitting the pilfered data to a remote server through a covert background process. Remarkably, the Trojan horse offers remote control capabilities, allowing manipulation from the command-and-control server (C&C server) to launch (D) DoS attacks on specified IP addresses. Notably, the Trojan horse showcases its efficacy as a cyber espionage tool by successfully aiding infiltration of Gmail and Facebook accounts. Its ability to operate persistently with zero-click adds an alarming dimension to its threat. Our experiments yield promising results advocating for the strength and discreet nature of our spyware tool that offers a comprehensive evaluation of Android OS security. The comparison results significantly exceed the performance of existing similar tools. Ultimately, our design will create awareness and enhance Android security.
Paper ID 26

GENERATIVE ARTIFICIAL INTELLIGENCE IN LATIN AMERICAN HIGHER EDUCATION: A SYSTEMATIC LITERATURE REVIEW

Maria Baldeon Calisto (Universidad San Francisco de Quito)*; Alejandra de la Torre Garcia (Universidad San Francisco de Quito)
mbaldeonc@usfq.edu.ec

The utilization of Artificial Intelligence (AI) and Generative AI (GenAI) in higher education has increased importantly in the last years. Studies show that AI holds promise in enhancing the learning experiences for both students and educators, offering personalized learning and assessment opportunities. This study conducts a systematic review on the application of AI within Latin American higher education. To this end, we synthesized 25 papers published between 2021 and 2023, encompassing AI’s utilization in Mexico, Colombia, Ecuador, Brazil, Peru, Chile, Argentina, and Bolivia. The analysis addresses three key inquiries: the prevalent applications of AI in Latin American education, the perceptions of AI and GenAI models among educators and students, and the particular challenges encountered by Latin American institutions in AI implementation. This systematic review offers an updated understanding of AI’s role in Latin American higher education, with a particular emphasis on the latest AI technologies.

Paper ID 28

HANDLING IMBALANCED DATA FOR DETECTING SCAMS IN ETHEREUM TRANSACTIONS USING SAMPLING TECHNIQUES

Lakshmi Priya Krishnan (University of North Florida); Iman Vakilinia (University of North Florida)*; Sandeep Reddivari (University of North Florida); Sanjay Ahuja (University of North Florida)
i.vakilinia@unf.edu

Blockchain technology and cryptocurrencies have captured global attention due to their numerous and versatile features, resulting in several industries and services adopting cryptocurrencies as payment methods. The advantages including user anonymity, open source, and tamper-proof transactions, have contributed to its popularity. However, these advantages have also attracted scammers who exploit the technology's features to engage in fraudulent activities, leading to a growth in crypto-frauds. To prevent and identify these frauds, various detection and prevention methodologies have been proposed, mainly using machine learning algorithms to identify scams as anomalies or outliers. The performance of such models depends on the datasets used and the features engineered. Often, these models face the challenge of having limited amounts of data that are scam-labeled. Under such circumstances, the model performs poorly due to an imbalanced dataset. Similarly, the features engineered and selected to train the model are also very important in detecting scams. With the help of sampling techniques, we propose to create a dataset that is research-ready and addresses the data imbalance problem. Additionally, we list the resources that can be used to collect labeled data. Furthermore, we discuss the practical significance of features and various feature engineering strategies in detecting scams from transactions in Ethereum.

Paper ID 32

CHAOS-BASED STREAM CIPHERS FOR 5G INTER-SLICE NETWORK SECURITY

Vismaya Vijayan (Amrita Vishwa Vidyapeetham)*
vismayanair2504@gmail.com

5G technology has transformed wireless communication networks, offering faster speeds, enhanced capacity, and seamless connectivity for numerous devices. An integral feature, network slicing, segments the infrastructure into distinct virtual networks called 'slices' tailored to diverse applications. Intra-slice and inter-slice domains play crucial roles in shaping 5G’s flexibility and adaptability. Ensuring the security of slice networks is paramount, especially against potential threats leveraging vulnerabilities within other slices, falling within the realm of the inter-slice domain. To address this concern, cryptography-based solutions have been implemented. This paper introduces an innovative Chaos-based encryption scheme firmly grounded in chaos theory, specifically tailored for enhancing inter-slice domain security.
security. It leverages chaotic maps, specifically the 2-Dimensional Logistic Sine Coupling Map, for key stream generation, combined with the lightweight ChaCha20 stream cipher for encryption. This fusion guarantees data confidentiality and security during transmission, in resource-limited settings, focusing primarily on enhancing the security posture within the inter-slice domain. The paper meticulously conducts a comprehensive security analysis of the proposed scheme and conducts performance comparisons with alternative encryption methodologies utilizing Baker’s map and Arnold’s cat map for key stream generation.

**Paper ID 33**

**COMPARATIVE ANALYSIS OF AUTOMATED SCANNING AND MANUAL PENETRATION TESTING FOR ENHANCED CYBERSECURITY**

Anna Qureshi (University of Bradford)*; Nikhil Rane (Student); Nikhil Rane (University of Bradford)
a.qureshi19@bradford.ac.uk

Web platform security has become a significant concern in the current cyber world. Adversaries constantly advance their skills and technologies to bypass modern cyber defence techniques to lure website vulnerabilities. In the cyber world, finding and mitigating vulnerabilities on the website is essential to avoid any damage to the organization. Two key techniques - vulnerability assessment and penetration testing - play a crucial role in identifying and mitigating these weaknesses. While vulnerability assessment scans the platform, revealing potential flaws, penetration testing goes a step further, simulating real-world attack scenarios to assess their true exploitability and possible damage. This paper compares automated scanning and manual penetration testing to evaluate the effectiveness of these techniques in uncovering vulnerabilities. The experimental results confirm that manual penetration testing is more effective than automated testing in terms of accuracy. Additionally, practical studies highlight the importance of a penetration tester's skills and experience in identifying and exploiting security weaknesses. Automated tools may also generate false positive results.

**Paper ID 34**

**ANDROPACK: A HYBRID METHOD TO DETECT PACKED ANDROID MALWARE WITH ENSEMBLE LEARNING**

Saranya Chandran (Amrita Vishwa Vidyapeetham)*; Mithun M (Amrita Vishwa Vidyapeetham)
saranyac@am.amrita.edu

In the rapidly evolving landscape of mobile security, the increasing risk posed by Android malware is a paramount concern. The inherent openness of the Android system emphasizes the critical need for continuous vigilance and strategic alertness. Packed malware poses a significant challenge in detection and analysis, as these deliberate techniques complicate traditional security measures, allowing malicious actors to conceal their intent effectively. This research proposes an automated system that integrates static and dynamic analysis, leveraging sophisticated methods to extract pertinent features from the APK. Additionally, this research incorporates an ensemble learning framework to enhance the robustness and accuracy of the analysis. The proposed system comprehensively examines the complexities of packed Android malware, thereby increasing detection accuracy by 95% and reinforcing the security infrastructure in mobile environments, addressing the dynamic nature of mobile threats.

**Paper ID 35**

**ANALYZING INSIDER CYBER THREATS AND HUMAN FACTORS WITHIN THE FRAMEWORK OF AGRICULTURE 5.0**

Kossi D Bissadu (UNT); Gahangir Hossain (University of North Texas)*; Leela Pavani Velagala (University of North Texas); Salleh Sonko (University of North Texas)
gahangir@gmail.com
In the transition to Agriculture 5.0, emphasizing human-machine interactions, the agricultural industry faces a heightened risk of cybersecurity threats stemming from human vulnerabilities. This study emphasizes the necessity of addressing human factors to ensure a balanced approach to technological advancement and cybersecurity in Agriculture 5.0. Specifically, it delves into insider threats as a significant human factor affecting agricultural cybersecurity, exploring diverse insider types and the associated security risks. The paper proposes preventive strategies grounded in the analysis of human factors to enhance security measures, safeguarding critical and sensitive agricultural information. Utilizing use case diagrams, Unified Modeling Language, function allocation, and task analysis, the study highlights various insider threats and their defense mechanisms within the context of Agriculture 5.0.

Paper ID 36

WHY PHISHING EMAILS ESCAPE DETECTION: A CLOSER LOOK AT THE FAILURE POINTS

Arifa Islam Champa (Idaho State University)*; Md Fazle Rabbi (Idaho State University); Minhaz Fahim Zibran (Idaho State University)
arifaislamchampa@isu.edu

This research uncovers why phishing emails often escape machine learning (ML) detection algorithms. For training and testing ML algorithms in detecting phishing emails, we produce and publicly release 11 curated datasets consisting of 217,470 emails categorized and labeled as phishing and legitimate emails. Then, we perform a quantitative analysis to assess the effectiveness of five ML algorithms and confirm the suitability of our curated datasets. Through an in-depth analysis of misclassified emails, we identify patterns indicating when ML fails to detect phishing emails. These findings inform the design and development of better phishing email filtering systems while our datasets will allow further studies in this direction.

Paper ID 37

A COMPREHENSIVE SPECTRUM OF OPEN PORTS

Rashad Aliyev (Khazar University)*
rashad@aliev.info

This paper explores enhancing user accessibility and experience in cybersecurity by introducing a user-friendly website interface for widely used port scanning tools (Nmap, Unicornscan, RustScan). Conducting global scans on the top 10 million hosts, the study provides valuable insights into open ports, vulnerabilities, and offers a foundation for future security strategies. The integration of this interface aims to make port scanning more accessible, bridging the gap between advanced cybersecurity tools and user-friendly interfaces, ultimately fortifying digital asset protection in an evolving threat landscape.

Paper ID 38

FEW-SHOT MULTI-LABEL MULTI-CLASS CLASSIFICATION FOR DARK WEB IMAGE CATEGORIZATION

Yagmur Aktas (VICOMTECH)*; Jorge Garcia (Vicomtech)
yaktas@vicomtech.org

Categorizing dark web image content is critical for identifying and averting potential threats. However, this remains a challenge due to the nature of the data, which includes multiple co-existing domains and intra-class variations. While many methods have been proposed to classify this image content, multi-label multi-class classification remains underexplored. In this paper, we propose a novel and efficient strategy for transforming a zero-shot single-label classifier into a few-shot multi-label classifier. This approach combines a label empowering methodology with few-shot data. We use CLIP, a conservative learning model that uses image-text pairs, to demonstrate the effectiveness of our strategy.

Finally, we compare our method's performance with other multi-label methodologies applied to CLIP and other leading multi-label architectures.
Paper ID 39
SMARTPHONE FORENSICS: A COMPARATIVE STUDY OF COMMON MOBILE PHONE MODELS
Abduljalil Alblooshi (Zayed University); Naser Aljneibi (Zayed University); Farkhund Iqbal (Zayed University); Richard Adeyemi Ikuesan (Zayed University); Zainab Khalid (National University of Sciences and Technology)*
zkhalid.msis18seecs@seecs.edu.pk

Smartphones are the most extensive repositories of user profile data such as activities related to personal and professional lives, working habits, and navigation histories. This stems from their rising inflow and pervasiveness. While some data may be retrieved quickly and simply, other (deleted) data may require the employment of cutting-edge forensic investigative tools. Smartphone applications, build on complex architectures (APIs, servers, storage, and cloud, etc.), typically require the use of specialized tools to gather, segregate, assess, analyze, and report on data, making acquisition and analysis more complex and time-consuming. This paper highlights the challenges of smartphone forensics while testing a range of Operating Systems (OSs) including Android, iOS, and Windows for the extraction of forensic artifacts. The results of both logical and physical acquisitions are presented. Depending on the data, extractions may also include methods such as installing an OS on the current server via a file transfer.

Paper ID 40
A COMPARATIVE ANALYSIS OF VISION TRANSFORMERS AND CONVOLUTIONAL NEURAL NETWORKS IN CARDIAC IMAGE SEGMENTATION
Maria Baldeon Calisto (Universidad San Francisco de Quito)*; Sebastian Granizo (Universidad San Francisco de Quito); Milena Iñiguez (Universidad San Francisco de Quito); Danny Navarrete (Universidad San Francisco de Quito); Daniel Riofrío (Universidad San Francisco de Quito); Noel Pérez-Pérez (Universidad San Francisco de Quito); Diego Benítez (Universidad San Francisco de Quito); Daniel Riofrío (Universidad San Francisco de Quito); Ricardo Flores-Moyano (Universidad San Francisco de Quito)
mbaldeonc@usfq.edu.ec

In recent years, Convolutional Neural Networks (CNNs) and Vision Transformers (ViTs) have emerged as dominant automated cardiac image segmentation methods. CNNs are efficient architectures that capture local spatial patterns, while ViTs can model long-range global dependencies. Each network has shown to provide better performance in certain types of tasks and datasets. In this work, we conduct a comparative analysis between ViTs and CNNs in the context of cardiac image segmentation. We statistically assess the performance of five CNNs and ViTs architectures using the publicly available Automated Cardiac Diagnosis Challenge (ACDC) MRI dataset. Employing a one-way ANOVA and Tukey’s test, our analysis indicates that CNNs exhibit superior performance compared to Transformers in segmenting the right ventricle cavity, left ventricle cavity, and left ventricle myocardium. Furthermore, CNN architectures tend to be smaller and easier to train. Among all networks under consideration, LinkNet achieves the highest performance with a mean dice of 0.8965 and a mean ASSD of 0.2960.

Paper ID 41
THE TRAJECTORY OF ROMANCE SCAMS IN THE U.S.
LD Herrera (Dakota State University)*; John Hastings (Dakota State University)
ld.herrera@trojans.dsu.edu

Romance scams (RS) inflict financial and emotional damage by defrauding victims under the guise of meaningful relationships. This research study examines RS trends in the U.S. through a quantitative analysis of web searches, news articles, research publications, and government reports from 2004-2023. This is the first study to use multiple sources for RS trend analysis. Results reveal increasing public interest and media coverage contrasted by a recent decrease in incidents reported to authorities. The frequency of research dedicated to RS has steadily grown but focuses predominantly on documenting the problem rather than developing solutions. Overall, findings suggest RS escalation despite declining official reports, which are likely obscured by low victim reporting rates. This highlights the need for
greater awareness to encourage reporting enabling accurate data-driven policy responses. Additionally, more research must focus on techniques to counter these crimes. With improved awareness and prevention, along with responses informed by more accurate data, the rising RS threat can perhaps be mitigated.

Paper ID 42

**OPINIONS EVOLUTION ANALYSIS IN TIME-VARYING SOCIAL NETWORKS: A SILENT SPIRAL OPINION MODEL**

Shan Liu (Communication University of China)*; Hanfei Zhao (Communication University of China)

liushan@cuc.edu.cn

The spiral of silence theory originating from the mass media era can no longer adapt to the phenomenon of social media era. Opinions in social networks are so diverse that people have opportunities to voice their opinions and prevent isolation. In this paper, we focus on an interesting phenomenon: the generation of pseudo-opinions caused by the spiral of silence and its impact on interpersonal relationships. We propose a silent spiral opinion model (SSOM) to explore how this phenomenon affects opinion evolution, as well as interpersonal relationships. We model the spiral of silence in which silent agents are given pseudo-opinions. In addition, we propose a time-varying network topology updating algorithm based on triangle closure to investigate how the spiral of silence would affect interpersonal relationships. Finally, we conduct simulations and analysis in ER random networks, which are easy to vary in size and density and capture some of the essential features of social networks. The experimental results reveal that the network size and the evolution of opinions are independent of each other, but when the network size increases, people are more likely to be silent and more distant from each other. The intensification of the spiral of silence accelerates the convergence of opinions and makes it easier to reach a consensus, but it also leads to more alienation of people and a decrease in the global clustering coefficient of the network. This study contributes to a deeper understanding of opinion dissemination in social networks and provides an important reference for opinion prediction.

Paper ID 44

**EVALUATION OF DIFFERENT PASSIVE METHODS FOR LIVENESS DETECTION**

Marius Butz (Karlsruhe University of Applied Sciences); Matthias Wölfel (Karlsruhe University of Applied Sciences)

marius.butz@h-ka.de

The rapid development of face anti-spoofing techniques has resulted in a wide variety of techniques, making it difficult to make meaningful comparisons and choices among them. To shed light on this aspect this research delves into various passive methods that rely solely on the observation of the person in front of the camera. Our study encompasses the execution, examination, and comparative evaluation of these methodologies. Furthermore, we analyze various attacks and examine how different methods show their effectiveness in identifying and counteracting these deceptive maneuvers. To guarantee a fair assessment of detection performance, we introduce an independent dataset, which was not used during the training phase. Our results illuminate the strengths and weaknesses of current passive anti-spoofing methods, offering valuable insights for enhancing secure biometric authentication systems.

Paper ID 45

**ADVERSARIAL CROSS-LASER ATTACK: EFFECTIVE ATTACK TO DNNs IN THE REAL WORLD**

Hanyu Wu (University of Electronic Science and Technology of China); Ke Yan (University of Electronic Science and Technology of China)*; Peng Xu (University of Electronic Science and Technology of China); Bei Hui (University of Electronic Science and Technology of China); Ling Tian (University of Electronic Science and Technology of China)

kyan@uestc.edu.cn

Deep neural networks for image classification have been widely used to enhance user experience, but adversarial attacks continue to pose a threat to the security of deep neural networks related systems. To advance the development of more robust and secure models, research in this field is important. Laser attacks have overcome some issues of previous attacks. To enhance the laser-based attack strategy, we propose a novel physical adversarial attack method that optimizes cross-laser parameters using a Bayesian Optimization algorithm improved by contour detection technology.
Our method solves the problems of traditional laser-based methods including positioning, insufficient perturbation intensity, low optimization efficiency, lack of multi-angle robustness, and optical path continuity issues. Digital and physical experiments were implemented, and our method achieved an attack success rate of up to 86.24%. Our adversarial attacks pose new challenges and requirements for artificial intelligence security.

**Paper ID 46**

**DIGITAL FORENSICS ANALYSIS OF YOUTUBE, INSTAGRAM, AND TIKTOK ON ANDROID DEVICES: A COMPARATIVE STUDY**

Chiamaka J Femi-Adeyinka (Sam Houston State University)*; Nuri Kose (Sam Houston State University); Tosin Akinsowon (Sam Houston State University); Cihan Varol (Sam Houston State University)

cjf068@shsu.edu

This study presents a comprehensive digital forensics analysis of social media platforms, specifically YouTube, Instagram, and TikTok, conducted on two distinct Android devices: a OnePlus 7 Pro and a Motorola X4 smartphone. Our methodology involved dedicating one phone exclusively to content creation (posting), while the other was used for engagement activities (watching, liking, commenting, and direct messaging). This approach enabled us to simulate and analyze distinct user roles on these platforms effectively. Both application-based and browser-based interactions were carefully examined. Using Magnet Axiom, we captured and analyzed images of the devices to document user activities. Additionally, Android Debug Bridge (ADB) tools were employed to access and investigate the browser history databases on both phones. This paper discusses our findings, emphasizing the digital forensics analysis of these platforms, highlighting the differences and similarities in user interactions across these platforms, and the implications of using various devices and access methods.

**Paper ID 47**

**MOBILE FORENSIC INVESTIGATION: EXTRACTIONS AND CONNECTIVITY ISOLATION IN PHONES UTILIZING ESIM, iSIM TECHNOLOGY.**

Nurettin S SENOL (Sam Houston State University)*; Amar A Rasheed (Sam Houston State University); Narasimha Karpoo Shashidhar (Sam Houston State University)

nurettinsenol@shsu.edu

As mobile devices have become an essential part of our lives, the investigation and extraction of digital evidence from these devices have gained outstanding importance. This article examines the potential and problems that are currently facing the forensic investigation of embedded SIMs and integrated SIMs. Digital forensic investigators must comprehend the nuances of these SIM technologies and establish efficient procedures for retrieving key evidence given the growing adoption of eSIM and iSIM in mobile devices. This article seeks to offer insights into the analysis of these small but mighty components by probing the prospective methods and strategies for eSIM and iSIM forensics. The results of this study can help forensic specialists unlock new types of digital evidence and improve their capacity for investigation in the constantly changing field of mobile forensics.

**Paper ID 48**

**KEY EXCHANGE WITH DIFFIE-HELLMAN PROTOCOL AND COMPOSITE HASH-FUNCTION**

Manuel A Cardona-López (Instituto Politécnico Nacional)*; Juan Chimal-Eguía (Instituto Politécnico Nacional); Víctor Silva-García (Instituto Politécnico Nacional); Rolando Flores-Carapia (Instituto Politécnico Nacional)

mcardonal2022@cic.ipn.mx

For the secure transmission of symmetrically encrypted data, sharing not only the data but also its secret key is crucial. Therefore, an effective key exchange mechanism is essential for secure key transmission. The Diffie-Hellman key exchange protocol has traditionally served as a method for securely transmitting secret keys by generating session keys. It relays its security on the discrete logarithm problem and can be enhanced by combining it with other cryptographic tools. In this context, we propose a key exchange algorithm that incorporates composite Hash-functions. The shared key of the Diffie-Hellman protocol is used to construct 128 strings, each processed individually by a distinct composite
SHA-512 function a secret number of times. Each number represents a byte of the key intended for transmission. Consequently, the encrypted key is formed by concatenating 128 strings of 512 bits each. The results of the encrypted key show entropy values close to 7.9, even when the secret key exhibits numerical patterns. The proposed algorithm utilizes 1024-bit numbers for the secret key, prime, and generator. It does not require sharing additional parameters beyond the public parameters of Diffie-Hellman and the encrypted key. Additionally, for enhanced security, private values can be changed in every communication, albeit at the cost of increased time, approximately 10 ms.

**Paper ID 51**

**INVESTIGATING SOCIAL MEDIA INTERACTIONS ON EDGE AND CHROME BROWSERS**

Jeffrey D Berg (Sam Houston State University)*; Kubra Gundogan (Sam Houston State University); Cihan Varol (Sam Houston State University)

jeffreyberg10@comcast.net

This paper presents an in-depth digital forensic analysis of user interactions on popular social media platforms, including YouTube, Instagram, and TikTok, through the usage of Chrome and Edge web browsers in both their standard and private browsing modes. The research methodically creates scenarios that include actions such as liking, posting, viewing, commenting, sharing, and direct messaging. We investigate physical and virtual machine environments. Key to our analysis were two approaches: firstly, an examination of data preservation in local, session, and IndexedDB storage using the Developer Tools of the browsers; secondly, a thorough inspection of the contents in local storage directories using the Magnet Axiom tool. Despite employing private browsing modes, our findings were significant. The Magnet Axiom tool successfully extracted revealing user data, including posted content and usernames, from the specified local storage paths. The fact that data is kept in both browsing modes presents serious privacy issues. This paper clarifies these implications, particularly about social media interactions, and offers important insights into the limitations and effectiveness of current digital forensic practices.

**Paper ID 52**

**IDENTIFYING MALWARE FAMILY WITH STRING MATCHING ALGORITHMS BASED ON API CALLS AND ENTIRE STRINGS**

Kubra Gundogan (Sam Houston State University)*; Khushi Gupta (Sam Houston State University); Laura J Garland (Sam Houston State University); Cihan Varol (Sam Houston State University); Narasimha K Shashidhar (SHSU)

kxg067@shsu.edu

Malware is a growing concern for governments, organizations, and individuals, as it can corrupt or steal confidential or sensitive data. Although security software constantly identifies and blocks malware, adversaries can produce slightly altered variants within the same malware family by making minor alterations to the original. Although this makes it challenging for the system to detect, it also provides an opportunity to detect malware from the same family early since many of its strings remain similar. In this study, we apply three similarity algorithms to nine malware families to identify whether a malware string is from the same family. First, we extract the strings of each executable and divide these into API calls and entire strings. Next, we use the Jaccard Coefficient, Longest Common Subsequence (LCS), and N-gram algorithms to determine the optimal threshold to determine whether two malware strings belong in the same malware family or not. Finally, we determine that threshold values 26.84% for LCS, 28.02% for Jaccard, and 54.16% for N-gram are optimal for detecting similar strings within all malware families, and we conduct both within-family and cross-family analyses to substantiate our results. Our analysis shows that the N-gram algorithm achieves high accuracy rates of 91.16% for entire strings and 93.11% for API calls. Similarly, the Jaccard algorithm also demonstrates strong accuracy, with rates of 91% for entire strings and 91.68% for API calls. On the other hand, the LCS algorithm's accuracy is comparatively lower, with 83.78% for entire strings and 71.65% for API calls.
Paper ID 53

COMPARISON OF PRE-TRAINED MODELS FOR OPTIMIZED TRANSFORMER BASED QUESTION ANSWERING SYSTEM

Tunahan Gokcimen (Firat University); Bihter Daş (Firat University)*
bihterdas@gmail.com

This study delves into the evaluation and optimization of transformer-based models for question-answering systems, focusing on health-related inquiries. Utilizing a specialized dataset extracted from Wikipedia articles, transformer models, namely Bert-base-cased, Electra-base, Deberta-base, Xlm-roberta-base, Distilbert-base, and Albert-base, were scrutinized based on their F1 scores and exact match accuracy. Electra-base and Deberta-base exhibited notable performance, showcasing the significance of models equipped with denoising mechanisms and disentangled attention. The outcomes highlight the critical role of tailored model selection in specific domains, particularly within health-related contexts. Future research avenues may explore fine-tuning strategies and optimizations for health datasets, addressing challenges in medical information extraction and question-answering. This study contributes valuable insights to the natural language processing field, guiding advancements in transformer-based question-answering systems, especially in the health domain.

Paper ID 54

STRUCTURED NAMED ENTITY RECOGNITION (NER) IN BIOMEDICAL TEXTS USING PRE-TRAINED LANGUAGE MODELS

Pinar Savci (Arçelik A.S.); Bihter Daş (Firat University)*
bihterdas@gmail.com

The field of Natural Language Processing (NLP) has witnessed remarkable progress in recent years, particularly in the domain of biomedical text analysis. Named Entity Recognition (NER), a pivotal task in information extraction holds the key to deciphering and extracting structured information from unstructured biomedical texts. Accurate identification and classification of entities, such as DNA, proteins, cell types, cell lines, and RNA, are imperative for advancing our comprehension of complex biological systems. This paper presents a comprehensive exploration of the application of state-of-the-art pre-trained language models, including Bert-base-cased, Distilbert-base-cased, Albert-base-V2, Xlm-roberta-base, Ernie-2.0-base-en, and Conv-bert-base, for structured Named Entity Recognition in biomedical texts. The BioNLP2004 dataset, enriched with diverse entity types, forms the basis for our experiments. Our objectives encompass a thorough investigation into the effectiveness of different pre-trained language models for biomedical NER, an in-depth analysis of the challenges posed by the BioNLP2004 dataset, and a comparative evaluation of the selected models in terms of precision, recall, and F1 score. Additionally, we explore the impact of fine-tuning strategies on model performance. The insights gained from this research have the potential to advance the capabilities of language models in the biomedical domain, contributing to more efficient and precise biomedical text analysis. This work serves as a stepping stone toward the broader goals of bioinformatics and medical research. The paper concludes with a summary of findings and outlines potential avenues for future research.

Paper ID 55

TOPIC MODELLING USING BERTOPIC FOR ROBUST SPAM DETECTION

Tunahan Gokcimen (Firat University); Bihter Daş (Firat University)*
bihterdas@gmail.com

Spam emails continue to be a challenging issue in terms of cybersecurity. This study uses state-of-the-art techniques such as BERTopic and various text-mining strategies to effectively address this issue. The study also compared the performance of four different embedding models in topic modeling. In particular, the experimental results underline
the outstanding performance of the “Roberta-base” model and highlight its effectiveness in detecting spam emails. The importance of this study lies in its role in demonstrating the effectiveness of BERTopic and related methodologies in combating spam emails, providing valuable information to researchers and practitioners on email security, natural language processing, and machine learning. The study’s comprehensive examination of spam datasets, combined with rigorous comparative analyses of placement patterns, advances the existing knowledge base in this area.

Paper ID 56

MULTI-LABEL CLASSIFICATION IN TEXT DATA: AN EXAMINATION ON INNOVATIVE TECHNOLOGIES

Pınar Savcı (Arçelik A.Ş.); Bihtrer Daş (Fırat University)*
bihterdas@gmail.com

This study focuses on examining the effectiveness of multi-label text classification methods in the field of innovative technology. Experimental results using four different transformer models such as bert-base-cased, albert-base-v2, xlm-roberta-base and bart-base reveal in detail the performance of these models on performance measures such as accuracy, F1 score and processing time. The study highlights another critical factor in model selection, the balance between accuracy and processing time, providing researchers and practitioners with valuable information on the selection of models suitable for specific use scenarios. Key findings of the study include bert-base-cased standing out with high accuracy and F1 score, while xlm-roberta-base stands out with competitive performance and improved processing efficiency. These results evaluate the success of transformer models in multi-label text classification tasks and reveal the factors to be considered in choices in this field. The study provides a framework for future research, guiding future studies on topics such as model discovery, development of fine-tuning strategies, and model interpretability.

Paper ID 58

ABUSEGPT: ABUSE OF GENERATIVE AI CHATBOTS TO CREATE SMISHING CAMPAIGNS

Ashfak Md Shibli (Tennessee Tech University); Mir Mehedi A Pritom (Tennessee Technological University)*; Maanak Gupta (Tennessee Technological University)
mpritom@tntech.edu

SMS phishing, also known as ‘smishing’, is a growing threat that tricks users into disclosing private information or clicking into URLs with malicious content through fraudulent mobile text messages. In recent past, we have also observed a rapid advancement of conversational generative AI chatbot services (e.g., OpenAI’s ChatGPT, Google’s BARD), which are powered by pre-trained large language models (LLMs). These AI chatbots certainly have a lot of utilities but it is not systematically understood how they can play a role in creating threats and attacks. In this paper, we propose AbuseGPT method to show how the existing generative AI-based chatbot services can be exploited by attackers in real world to create smishing texts and eventually lead to craftier smishing campaigns. To the best of our knowledge, there is no pre-existing work that evidently shows the impacts of these generative text-based models on creating SMS phishing. Thus, we believe this study is the first of its kind to shed light on this emerging cybersecurity threat. We have found strong empirical evidences to show that attackers can exploit ethical standards in the existing generative AI-based chatbot services by crafting prompt injection attacks to create newer smishing campaigns. We also discuss some future research directions and guidelines to protect the abuse of generative AI-based services and safeguard users from smishing attacks.

Paper ID 59

DELETED FILE RECOVERY FOR THE LINUX FILE SYSTEM (EXT4): FINDING THE STATE-OF-THE-ART

Sai Bharadwaj Srirvaram (Bowling Green State University)*; Sankardas Roy (Bowling Green State University)
ssaubha@bgsu.edu

In a digital forensics investigation, deleted file recovery (DFR) can play a critical role. Apart from forensic investigation scenarios, DFR can also benefit a regular user if she wants to recover an important file that she has unintentionally deleted. Currently, Linux OS is quite popular and it uses Ext4 as its default file system. Prior researchers investigated
DFR capability of digital forensics (DF) tools for Windows machines that use FAT and NTFS file systems. However, in most part, prior works did not investigate DFR capability of DF tools for Linux machines. In the current work, we attempt to fill in this gap by experimenting with the state-of-the-art DF tools to examine their DFR capability for Ext4. We found that only a few tools can recover or identify deleted files in Ext4 unless the deleted files contain special signatures. Furthermore, we have designed canonical file system images, and tested the DFR tools on these images to figure out what makes the tools succeed or fail. We report a gist of the results in the current paper.

**Paper ID 60**

**FORENSIC ANALYSIS OF AN IOT ARP SPOOFING ATTACK**

Sabrina Friedl (University of Regensburg)*; Günther Pernul (University of Regensburg)

sabrina.friedl@ur.de

The Internet of Things (IoT) creates numerous attack opportunities. Address Resolution Protocol (ARP) spoofing (or cache poisoning) attacks allow hackers to impersonate a PC and steal traffic. This attack is commonly used in spy movies and increasingly in IoT environments. To show the procedure of an IoT forensic analysis to an ARP spoofing attack, we simulate an IoT environment using Arduinos (UNO Rev2, NANO 33 IoT) and sensors (keypad module, motion sensor) acting as IoT devices in the network. This is the basis for the presented fictitious case scenario (based on an actual case), in which a former insider helps a hacking group to breach a corporate network and spy on company secrets to sell them to the competition (industrial espionage). This attack scenario increasingly used and possible by novel IoT attack paths damages customers’ trust in the company and leads to the loss of secret documents, directly causing significant financial loss for the company. The case scenario shows that forensic analysis can provide valuable evidence. It demonstrates the current danger of newly implemented IoT environments within companies and the dangerous use of standard IoT devices (devices available on the market and ones developed for pen-testing) as entry points for advanced attacks.

**Paper ID 61**

**LOAD CHARACTERIZATION OF AI APPLICATIONS USING DQoES SCHEDULER FOR SERVING MULTIPLE REQUESTS**

Taufiq Odhi Dwi Putra (Institut Teknologi Sepuluh Nopember)*; Royyana Muslim Ijtihadie (Institut Teknologi Sepuluh Nopember); Tohari Ahmad (Institut Teknologi Sepuluh Nopember)

6025221005@mhs.its.ac.id

In today's era, many types of Artificial Intelligence (AI)-based applications are being developed to fulfill a variety of needs, for example, counting objects recorded using a camera, identifying diseases by processing MRI images, and predicting traffic congestion levels at specific times. One way to provide infrastructure resources that match the workload of AI-based applications is to understand the patterns or characteristics of their workloads. Because an AI model is run using a Graphical Processing Unit (GPU), several parts of the AI model's architecture use Video Random Access Memory (VRAM) as temporary storage media to speed up the running time. This paper analyzes the characteristics of workloads from AI-based applications in terms of running time and VRAM usage, where experiments are conducted in two request scenarios: sequential request and concurrent request and using four types of AI models from the Super Resolution General Adversarial Network (SRGAN), namely no prune, random unstructured, L1 norm, and L2 norm. Based on the experimental results, the workload of all four types of SRGAN models will be almost the same when using the sequential request scenario, while in the concurrent request scenario, the four types of SRGAN models have different workloads. There are models that are more effectively processed one at a time rather than several at once, for example, in the SRGAN no prune model, and there are models that if processed several at once at the same time will be more effective compared to being processed one at a time, for example in the SRGAN random unstructured and L2 norm models."
**Paper ID 62**

**UNVEILING DIGITAL SECRETS: AN IMAGE TEXT VISION APP FOR ENHANCED DIGITAL FORENSICS INVESTIGATIONS**

Supriya S Bandal (University of Nevada, Reno)*; Suman Rath (University of Nevada, Reno)

sbandal@nevada.unr.edu

Digital forensics plays a pivotal role in uncovering crucial evidence from electronic devices, with Optical Character Recognition (OCR) standing out as a key technology for extracting text from images. This paper explores the challenges associated with OCR, including image quality, font variations, and contextual understanding. Despite its invaluable utility, the renowned digital forensics tool Autopsy currently lacks an inbuilt text extraction facility, presenting an opportunity for innovation. In response to this gap, our proposed novelty suggests integrating a dedicated text extraction module within Autopsy. While Autopsy excels in keyword searches, the addition of a text extraction feature would provide investigators with a comprehensive solution for analyzing textual content within digital image media. This paper concludes by emphasizing the significance of combining OCR with advanced forensic tools and highlights how enhancing Autopsy's capabilities aligns with the evolving demands of the digital forensic landscape. The suggested innovation positions Autopsy as a more robust and holistic tool, ensuring forensic practitioners can effectively navigate the complexities of digital evidence analysis. The open-source developed tool is available at: https://digital-forensics-text-vision.netlify.app/

**Paper ID 63**

**UNDERSTANDING MICROBENCHMARK DETECTION OF EXISTING EXPLOITS IN APPLE M1 AND M2 CHIPS**

Dr Richard Ward (University of South Wales); Thomas P Harris (University of South Wales)*

tom.harris@southwales.ac.uk

Understanding the causes, effects, and detection / mitigation methods of side-channel attacks (SCAs) is essential in providing a secure environment. Current studies into SCAs have focused on Intel microarchitecture and Apple Silicon chips (such as M1 and M2) have been left under-represented in the research literature. The aim of this paper is to identify a gap in microarchitectural research of M1 and M2 Apple chips. The long-term objective of this research is to apply the Unified Side Channel Attack – Model (USCA-M) four-phase testing process to identify the critical components used within the exploit and at a low-level catch the Hardware Performance Counter (HPC) events of M1 and M2 chips.

**Paper ID 67**

**EXPLORING SECURITY, PRIVACY, AND FORENSICS CONCERNS IN THE METAVERSE**

Sultan Althaqeel (NAUSS)*; Shema Alenazi (NAUSS); Sumaya Alshokeeran (NAUSS)

444000217@student.nauss.edu.sa

The notion of the “metaverse” has garnered considerable attention from professionals and scholars in various fields due to its potential to revolutionize how people engage with digital media, streamline workflows, and enhance interpersonal communication. With the use of advanced technologies, such as artificial intelligence and blockchain, the metaverse is transitioning from a mere idea in science fiction to an imminent reality. However, the metaverse is currently experiencing a multitude of cyberattacks, mainly due to its novel and complex infrastructure, which poses security, privacy, and forensic challenges. To address these issues, this paper employs a comprehensive methodology that involves conducting a literature review and analyzing the use case Virtual Verses. This paper aims to evaluate potential security, privacy, and forensic challenges in the metaverse. The outcomes of this paper will offer valuable perspectives for future scholars to explore the complexities and susceptibilities associated with privacy, security, and forensic

16
matters within the metaverse. This will facilitate the development of a comprehensive understanding of these challenges.

**Paper ID 69**

**BEHIND (DIGITAL CRIME) SCENES - AN MSC MODEL**

Mario Raciti (IMT School for Advanced Studies Lucca)*; Giampaolo Bella (University of Catania)
mario.raciti@imtlucca.it

Criminal investigations are inherently complex as they typically involve interactions among various actors like investigators, prosecutors, and defendants. The pervasive integration of technology in daily life adds an extra layer of complexity, especially in crimes that involve a digital element. The establishment of digital forensics as a foundational discipline for extracting digital evidence further exacerbates the complex nature of criminal investigations, leading to the proliferation of multiple scenarios.

Recognising the need to structure standard operating procedures for the handling of digital evidence, the representation of digital forensics as a protocol emerges as a valuable opportunity to identify security and privacy threats. In this paper, we delineate the protocols that compose digital forensics within a criminal case, formalise them as message sequence charts (MSCs), and identify their functional requirements.

**Paper ID 70**

**SECURING ARTIFICIAL INTELLIGENCE: EXPLORING ATTACK SCENARIOS AND DEFENSE STRATEGIES**

İrem Zehra Altun (TUBITAK BILGEM Cyber Security Institute)*; Abdurrahman Emre Ozkok (TUBITAK BILGEM Cyber Security Institute)
iremzehraaltun@gmail.com

In today's landscape, the widespread integration of artificial intelligence (AI) solutions across diverse domains has become commonplace. Yet, despite its omnipresence, AI applications often lack adequate protection, leaving them vulnerable to various threats. Consequently, businesses find themselves in need of clear guidance to navigate these risks effectively. This study aims to address this gap by shedding light on attacker activities targeting AI applications, offering robust defense mechanisms, and creating a comprehensive checklist for evaluating current processes. By analyzing attack and defense strategies, it is clear that although these methods are similar to those used in traditional information systems, their implementation in AI contexts differs significantly. This study provides detailed implementation insights and a security checklist to help organizations assess process maturity quickly. By identifying and addressing security gaps promptly, organizations can enhance the resilience of their AI infrastructure.

**Paper ID 71**

**A DIGITAL FORENSIC METHODOLOGY FOR ENCRYPTION KEY RECOVERY FROM BLACK-BOX IOT DEVICES**

Muhammad rusyaidi Bin zunaidi (University college dublin); Dr. Asanka P Sayakkara (University of Colombo School of Computing, Sri Lanka); Mark Scanlon (University College Dublin)*
mark.scanlon@ucd.ie

In an era where digital data security is becoming all-pervasive, and data encryption is baked in by default on many consumer-level and commercial-level devices, the encryption of Internet of Things (IoT) devices presents a significant obstacle for lawful digital forensic investigation. Towards addressing this issue, this paper introduces a novel digital forensic methodology that leverages electromagnetic side-channel analysis (EM-SCA) for the non-invasive recovery of encryption keys from black-box IoT devices, i.e., where little/nothing is known about the device's encryption in advance. By reducing the key space necessary for brute-force decryption and employing machine-learning techniques, the proposed approach enhances the digital forensic process – helping to mitigate investigative roadblocks and case backlogs. This automated, adaptable system not only preserves the integrity of forensic evidence, but also ensures wide
applicability within the evolving IoT landscape. This practical methodology could prove invaluable for investigators facing the complexities of encrypted device analysis encountered during their cases.

Paper ID 72

FORENSIC ANALYSIS OF WHATSAPP, INSTAGRAM, AND TELEGRAM ON VIRTUAL ANDROID DEVICE

Dina Millatina (UIN Sunan Kalijaga)*; Eko Hadi Gunawan (UIN Sunan Kalijaga); Bambang Sugiantoro (UIN Sunan Kalijaga)

21106050058@student.uin-suka.ac.id

Social media platforms such as WhatsApp, Telegram, and Instagram have rapidly grown in the daily lives of modern society, with significant impacts globally and in Indonesia. This research highlights the forensic role in investigating the use of social media on the Android platform, specifically focusing on WhatsApp, Telegram, and Instagram. The primary focus is on forensic analysis methodology, involving experiments in a virtual Android device environment using Genymotion. The identification of artifacts from these three applications reveals a high investigative value, emphasizing the importance of a profound understanding of data storage locations and potential security risks. While users can delete data from devices, this research underscores that the persistence of data on platform servers remains a challenge, and this deep understanding is crucial for digital forensic processes in investigation and recovery of relevant information.

Paper ID 73

LLM-BASED FRAMEWORK FOR ADMINISTRATIVE TASK AUTOMATION IN HEALTHCARE

Senay A Gebreab (Khalifa University); Khaled Salah (Khalifa University); Raja Jayaraman (Khalifa University)*; Muhammad Habib ur Rehman (King’s College London); Samer Ellahham (Cleveland Clinic and Cleveland Clinic Abu Dhabi)

raja.jayaraman@ku.ac.ae

Artificial Intelligence (AI) has been transformative in the healthcare sector, leading to precision in medical diagnosis, effective treatment options, and a significant improvement in patient safety. However, computer-based administrative tasks (such as retrieval of medical and health records, patient registration, medical billing, filing and documentation, and appointment scheduling) still impose a heavy burden on healthcare professionals, causing a reduced quality of care and efficiency. In light of these challenges, this paper proposes a large language model (LLM)-based multi-agent framework designed to automate some of the administrative work in clinical settings. In our proposed solution, these LLM agents coordinate to parse instructions, breakdown tasks, and execute a sequence of actions in a workflow. They are equipped to not only execute documentation process at the database level but also operate directly on web-based electronic medical record (EMR) platforms. Moreover, the framework integrates data sources through a retrieval-augmented generation (RAG) system to allow streamlined interaction with patient information and medical records, mediated through an agent interface. The framework is designed with security in mind to defend against malicious prompts. We demonstrate the practicality our solution by testing on various complex tasks that require the use of multiple tools and an EMR website. The result show the framework’s effectiveness in handling diverse administrative tasks.

Paper ID 74

RECOVERY CAT: A DIGITAL FORENSICS TOOL FOR CRYPTOCURRENCY INVESTIGATIONS

Lilita Infante (Crypto Asset Technology Labs); Roger A. Hallman (Crypto Asset Technology Labs)*; John Hayes (Crypto Asset Technology Labs); Evelyn Cronnon (Crypto Asset Technology Labs); Uri Stav (Crypto Asset Technology Labs)

Roger.A.Hallman@gmail.com

The increasing use of the Internet and cyber capabilities by criminals have made digital forensics a critical component of criminal investigations and prosecution. Criminal networks were early adopters of the cryptocurrency ecosystem; however, forensics capabilities for cryptocurrency-related investigations have been lacking. While investigators may utilize a number of commercially available digital forensics tools to search for cryptocurrency-related evidence, these tools are inadequate for the task. This paper presents Recovery CAT, a cryptocurrency specific forensics tool for finding
crypto artifacts such as seed phrases, addresses, private keys, wallet applications, hardware wallet usage, exchange domains, etc.

**Paper ID 75**

**A ROBUST MISBEHAVIOR DETECTION SYSTEM FOR COOPERATIVE DRIVING NETWORK**

Abdullahi Modibbo Abdullahi (Towson University); Wassila Lalouani (Towson university)*; Messaoud Rahim (University of MEDEA)

wlalouani@towson.edu

Cooperative Intelligent Transportation Systems (c-ITS) stand as visionary pillars in shaping the future landscape of vehicular networks. These systems hinge on the seamless orchestration of Vehicle-to-everything (V2X) communication, fostering the seamless exchange of vital information between vehicles and the underlying infrastructure. Within this intricate ecosystem, vehicles collaborate harmoniously, disseminating V2X messages throughout the network. However, the transmission of deceptive or inaccurate information by rogue vehicles has the potential to endanger road safety. Misbehavior Detection systems (MBS) perform plausibility and consistency checks on the received V2X information or consider machine learning models training while ignoring the variability of the traffic over time. In this paper, we introduce a stacked meta-learning model for misbehavior detection, leveraging time-series V2X data to distinguish between genuine and aberrant exchanged information. Our proposed approach integrates predictions from various probabilistic learning models, incorporating them into a CNN-LSTM meta-learner to weigh the outputs of the probabilistic classifiers for accurate misbehavior detection. Our method demonstrates its ability to identify a wide range of faults and attacks, including those associated with rare types of attack, by learning the inherent data distribution and essential characteristics of network traffic. Simulation results reveal that the proposed model not only outperforms prominent MBS in the literature by accurately identifying various forms of misbehavior within cooperative driving systems but also reduces the overall execution time of aberrant behavior detection.

**Paper ID 77**

**MULTIMEDIA FORENSICS: PRESERVING VIDEO INTEGRITY WITH BLOCKCHAIN**

Oluwasola Mary Adedayo (The University of Winnipeg)*; Sahilkumar Ahir (The University of Winnipeg)

m.adedayo@uwinnipeg.ca

This paper addresses some of the challenges of video forgery detection in multimedia forensics. It presents a solution that enhances video verification by utilizing the non-alterable features of blockchain technology and video hashing algorithms. The proposed approach is applicable in different application areas and can be used to increase video credibility, identify manipulations, and improve the storage process of tracking changes to video data. The paper describes our experiments and results of the proposed solution for video integrity preservation and verification, providing an alternative way to the quality assurance and security of video content in different industries.

**Paper ID 79**

**UNRAVELING IOT TRAFFIC PATTERNS: LEVERAGING PRINCIPAL COMPONENT ANALYSIS FOR NETWORK ANOMALY DETECTION AND OPTIMIZATION**

Bradley A Boswell (Augusta University)*; Seth Barrett (Augusta University); Gokila Dorai (Augusta University)

brboswell@augusta.edu

This paper presents a novel approach to analyzing IoT traffic patterns using Principal Component Analysis (PCA) on traffic captures from multiple IoT devices. The increasing adoption of IoT devices has led to growing concerns about their security and the need for efficient methods to detect anomalies in network traffic. In this study, we employ PCA to identify key patterns and reduce the dimensionality of the IoT traffic data, enabling a more streamlined and efficient analysis. The advantages of using PCA in this context include its capability to identify hidden correlations in traffic data, reduce noise, and improve the detection of anomalies. By applying PCA to IoT traffic data, we demonstrate its effectiveness in detecting unusual traffic patterns and potential security threats. This research contributes to the
development of advanced edge-based detection mechanisms, which can be crucial for securing IoT devices and networks. As edge computing becomes more prevalent, the ability to detect and mitigate risks at the network periphery is essential for maintaining the overall security of IoT ecosystems. Our findings highlight the potential of PCA as a valuable technique for enhancing edge-based detection methods, thereby contributing to a more robust and secure environment for IoT devices and their users.

Paper ID 80

SECURING HEALTHCARE 5.0: EXPLORING BYOD CYBER RISKS, MISUSE CASES, AND BEST PRACTICES

Durga Srikari Maguluri (University of North Texas); Leela Pavani Velagala (University of North Texas); Gahangir Hossain (University of North Texas)*

gahangir@gmail.com

The increasing prevalence of personal devices, such as smartphones and tablets, in healthcare settings has prompted healthcare professionals to frequently utilize their own devices for accessing patient records and engaging in communication with colleagues and patients, commonly referred to as Bring Your Own Device (BYOD). Despite the advantageous aspects of this trend, such as immediate patient care, personalized healthcare solutions, and the digitization of healthcare, it also introduces notable cybersecurity risks from both insiders and outsiders. This paper delves into the investigation of the role of BYOD devices in fostering cybersecurity awareness and its correlation with the productivity of healthcare professionals. The research addresses the inquiry surrounding the impact of cybersecurity awareness on enhancing the productivity of healthcare professionals. To comprehend potential cyber risks and their effects on the productivity of healthcare professionals, we conduct a thorough examination through a comprehensive literature review and analysis of misuse cases. Furthermore, we put forth best practices for healthcare organizations in crafting a secure Healthcare 5.0 framework that incorporates BYOD security. According to our findings, effective security training for healthcare professionals can result in a substantial reduction in cyber threats. Moreover, this study recommends the establishment of a robust cybersecurity framework to mitigate risks across all levels of critical infrastructural assets in the healthcare sector.

Paper ID 82

STREAM CLUSTERING ON A FORENSIC TIMELINE

Deka Julian Arrizki (Institut Teknologi Sepuluh Nopember); Stefanus Albert Kosim (Institut Teknologi Sepuluh Nopember); Hudan Studiawan (Institut Teknologi Sepuluh Nopember)*

hudan@its.ac.id

Digital forensics heavily relies on forensic timelines to maintain a chronological record of events and activities. With the exponential growth of digital activity, it is a significant challenge to efficiently categorize related events on these timelines. Inefficient memory utilization is the primary challenge, as forensic timelines encompass large and complex data, causing the capability to process data incrementally. This paper introduces an innovative approach that employs stream clustering techniques for event segmentation and categorization within forensic timelines. It considers forensic timelines as dynamic data streams that adapt in real-time to incoming events. This approach optimizes the processing and grouping of emerging events by leveraging temporal patterns and evolving event contexts, unlike traditional clustering methods that require complete datasets. In this study, three-stream clustering algorithms were tested, and it was discovered that link clustering produced the lowest score in silhouette score and Davies-Bouldin Index with the highest score in Calinski-Harabasz Index compared to DenStream and BIRCH. This concluded that link clustering performs the best clustering among these three algorithms.

Paper ID 86

EVALUATION OF PRIVACY-UTILITY TRADEOFF IN GENERATIVE ADVERSARIAL NETWORK VARIANTS

Shahnewaz karim Sakib (University of Tennessee at Chattanooga)*; Tomojit Ghosh (University of Tennessee at Chattanooga)

ssakib1@utc.edu
In this digital-driven world, data privacy is of utmost importance, encompassing both individual and corporate needs. Data owners need to share their data to ensure that users can derive utility from it. However, releasing data in its original form can pose several privacy risks. One viable solution is to generate synthetic datasets based on the original data, ensuring that they can provide similar utility while mitigating privacy concerns. Various methods have been adopted to generate synthetic data, with the use of Generative Adversarial Networks (GANs) being the most popular approach. In this paper, we have generated synthetic data using different GAN variants and evaluated their performance in terms of the privacy-utility trade-off. We compared these GAN variants against the baseline case, where the data was released in its original form, and the Gaussian copula method, which models the dependence structure between multiple variables. Our analysis indicates that the use of Conditional GAN (CTGAN) is the most effective approach for generating synthetic datasets to tackle the privacy-utility trade-off problem.

Paper ID 87
SECURITY AND PRIVACY THREATSPOSED BYIOT DEVICES USED BYSTUDENTS ON COLLEGE CAMPUS
Hala Strohmier (University of South Carolina)*
hala.strohmier@usca.edu

The increasing use of Internet of Things (IoT) devices on college campuses has significantly changed how students go about their daily lives. This surge of IoT brings potential security and privacy risks. This research focuses on understanding the IoT landscapes at the University of South Carolina Aiken (USCA), investigating vulnerabilities, and determining the need for improved security awareness. By combining survey data, network live scanning data, network monitoring, and simulated attacks, our analysis revealed a wide range of devices on the campus, suggesting possible security risks. Using the tool PRET exposes vulnerabilities in common devices, showing the need for direct security measures. Additionally, we explored wireless network vulnerabilities through capturing and decrypting WPA handshakes. The study showed common issues in IoT security, such as default credentials and network vulnerabilities. The conclusions underscore the need for a careful balance between the benefits of IoT and the need for increased security measures.

Paper ID 88
HNMBLOCK: BLOCKCHAIN TECHNOLOGYPOWERED HEALTHCARE NETWORK MODEL FOR EPIDEMIOLOGICAL MONITORING, MEDICAL SYSTEMS SECURITY, AND WELLNESS
Naresh Kshetri (Emporia State University)*; Rahul Mishra (University of Allahabad); Mir Rahman (Emporia State University); Tanja Steigner (Emporia State University)
NKshetri@emporia.edu

In the ever-evolving healthcare sector, the widespread adoption of Internet of Things and wearable technologies facilitates remote patient monitoring. However, the existing client/server infrastructure poses significant security and privacy challenges, necessitating strict adherence to healthcare data regulations. To combat these issues, a decentralized approach is imperative, and blockchain technology emerges as a compelling solution for strengthening Internet of Things and medical systems security. This paper introduces HNMblock, a model that elevates the realms of epidemiological monitoring, medical system security, and wellness enhancement. By harnessing the transparency and immutability inherent in blockchain, HNMblock empowers real-time, tamper-proof tracking of epidemiological data, enabling swift responses to disease outbreaks. Furthermore, it fortifies the security of medical systems through advanced cryptographic techniques and smart contracts, with a paramount focus on safeguarding patient privacy. HNMblock also fosters personalized healthcare, encouraging patient involvement and data-informed decision-making. The integration of blockchain within the healthcare domain, as exemplified by HNMblock, holds the potential to revolutionize data management, epidemiological surveillance, and wellness, as meticulously explored in this research article.
Paper ID 89

CYBERSECURITY DATA VISUALIZATION: DESIGNING A COURSE FOR FUTURE HIGH SCHOOL STUDENTS SHAFI PARVEZ

Mohammed (University of North Texas); Gahangir Hossain (University of North Texas)*; Syed Yaseen Quadri Ameen (University of North Texas)
gahangir@gmail.com

To keep pace with modern technological advancements, school education is embracing advanced computing curricula, which encompass disciplines such as data science, artificial intelligence (AI), machine learning (ML), and cybersecurity. Understanding complex information can be facilitated through data visualization techniques. Integrating tools such as Tableau into high school curricula can enhance students’ analytical and visual comprehension skills. This paper offers a comprehensive framework for delivering effective data visualization education using Tableau in high school settings. It emphasizes the significance of data visualization, explores Tableau's utility as a pedagogical tool, outlines strategies for curriculum integration, and assesses its impact on student learning outcomes. Additionally, the paper addresses challenges and provides guidance for educators implementing Tableau-based data visualization in secondary education.

Paper ID 91

ENHANCED UAV SECURITY: OPTIMIZING ACCURACY AND EFFICIENCY WITH MSBCE FEATURE SELECTION

Tomojit Ghosh (University of Tennessee at Chattanooga)*; Shahnewaz Sakib (University of Tennessee at Chattanooga)
tomojit-ghosh@utc.edu

The proliferation of Unmanned Aerial Vehicles (UAVs) has brought about transformative advancements across industries, accompanied by new security challenges. This study introduces a novel approach to detecting intruder signals in UAVs using sparsity-based machine-learning techniques. Utilizing the Masked Sparse Bottleneck Centroid-Encoder (MSBCE), an artificial neural network-based feature selection model, we conducted feature pruning on manually derived features from raw WiFi traffic signals. Remarkably, leveraging MSBCE enabled us to achieve exceptional prediction accuracy of $100\%$ across five diverse UAV datasets, even with a sparse feature subset of merely one to two features. This breakthrough promises faster runtime predictions and reduced resource usage (CPU time and memory) on smaller devices, owing to the compact UAV feature set determined by MSBCE. Building on MSBCE’s proven effectiveness in high-dimensional biological and big datasets, this study highlights its potential as a state-of-the-art feature selection model in UAV security applications. Through this work, we aim to drive advancements in UAV security, fostering safer and more secure deployment of UAV technology across various domains.

Paper ID 94

ECONOMETRIC AND AI-BASED MODELLING OF NIGERIA’S INTEREST RATES BASED ON FISHER EQUATION

Sagiru Mati (Near East University)*; Salim Ibrin Danbatta (Uskudar University); Asaf Varol (The University of Tennessee at Chattanooga); Ahad Nasab (UT Chattanooga); Abdullahi Garba Usman (Near East University); Berna Uzun (Near East University); Ahmad Nuhammad (Firat University)
sagirumati@gmail.com

In this study, linear and non-linear models are employed to model Central Bank Rate, Deposit Interest Rate, Lending Rate and Treasury Bill Rate. The choice of variables is guided by Fisher Equation. The linear models range from Autoregressive Integrated Moving Average, Simple Linear Regression, Autoregressive Distributed Lag model, Vector Autoregressive model, Bayesian Vector Autoregressive model to Vector Error Correction Model (VECM). The non-linear models include Artificial Neural Network and Adaptive Neuro-Fuzzy Inference System (ANFIS). The results show that VECM outperforms other models in the testing sub-sample, while ANFIS produces the highest forecast
accuracy in the training sub-sample. Ensembling the VECM and ANFIS produces the best forecast accuracy for both the sub-samples. The results of this study can serve as a reference for modelling interest rates and provide the benchmark for investment decisions and macroeconomic policy designs.

Paper ID 95

DEMYSTIFYING KNITR PACKAGE: ESSENTIAL RECIPES AND EASY STEPS FOR ADDING KNIT-ENGINES IN R

Sagiru Mati (Near East University)*; Irfan Civcir (Ankara University); Salim Jibrin Danbatta (Uskudar University); Asaf Varol (The University of Tennessee at Chattanooga); Ahad Nasab (UT Chattanooga); Ahmad Nuhammad (Firat University); Sani I Abba (King Fahd University of Petroleum & Minerals, Dhahran, 31261, Kingdom of Saudi Arabia.)
sagirimati@gmail.com

The knitr package provides an avenue for incorporating programming languages and statistical applications into R Markdown and Quarto document for the sake of reproducibility. However, deep technical knowledge of R programming is required to achieve this task. In addition to this, the existing literature does not provide a guide on how to add econometric/statistical programs such as EViews, gretl, and Dynare. This paper develops and explains four easy steps for adding econometric/statistical applications by taking into account their peculiarities. The recipes provided in this paper can be useful in enhancing the reproducibility, accuracy, and reliability of econometric/statistical computations. The recipes can also be used in cooking new knit-engines or modifying the existing ones.

Paper ID 97

A REVIEW OF ADVANCEMENTS AND APPLICATIONS OF PRE-TRAINED LANGUAGE MODELS IN CYBERSECURITY

Zefang Liu (Georgia Institute of Technology)*
liuzefang@gatech.edu

In this paper, we delve into the transformative role of pre-trained language models (PLMs) in cybersecurity, offering a comprehensive examination of their deployment across a wide array of cybersecurity tasks. Beginning with an exploration of general PLMs, including advancements and the emergence of domain-specific models tailored for cybersecurity, we provide an insightful overview of the foundational technologies driving these developments. The core of our review focuses on the multifaceted applications of PLMs in cybersecurity, ranging from malware and vulnerability detection to more nuanced areas like log analysis, network traffic analysis, and threat intelligence, among others. We also highlight recent strides in the application of large language models (LLMs), showcasing their growing influence in enhancing cybersecurity measures. By charting the landscape of PLM applications and pointing toward future directions, this work serves as a valuable resource for both the research community and industry practitioners, underlining the critical need for continued innovation and exploration in harnessing PLMs to fortify cybersecurity defenses.

Paper ID 99

DNS TUNNEL PROBLEM IN CYBERSECURITY

Güneş Gürsoy (Maltepe University)*; Asaf Varol (The University of Tennessee at Chattanooga); Ahad Nasab (UT Chattanooga)
gunesgursoy@hotmail.com

The Domain Name System (DNS) is the most important building block of the Internet. Websites, file transfer applications, and e-mail services use the DNS service. Therefore, these services can rarely be blocked by firewalls to prevent their access from being affected. Since applications such as firewalls and Intrusion Detection Systems (IDS) do not check the allowed protocols, attackers can open a secret path called DNS Tunnel through the DNS protocol to access sensitive data and cause many attacks. In this study, DNS Tunnel, DNS Tunnel detection methods and detection methods, and DNS attack types are included.
Cyber Ready Rural: Understanding Law Enforcement Cyber Readiness

Lucy Tsado (Lamar University); Camille Gibson (Prairie View A&M University); Izzat Alsmadi (Texas A&M University)*; Janaya Bob (Lamar University)

ialsmadi@tamusa.edu

As rural communities increasingly become interconnected through digital platforms, law enforcement agencies face unprecedented challenges in safeguarding their jurisdictions against cyber threats. This study delves into the concept of "Cyber Ready Rural," examining the cyber readiness of law enforcement agencies operating in rural settings. The research explores the unique dynamics, constraints, and opportunities that shape the cybersecurity landscape in rural areas, emphasizing the need for tailored strategies to enhance law enforcement’s preparedness for cyber threats. Ultimately, the study aspires to offer actionable recommendations that empower rural law enforcement agencies to navigate the evolving cyber landscape effectively. By fostering a deeper understanding of the challenges and opportunities inherent in securing rural communities against cyber threats, this research aims to assist policymakers, law enforcement leaders, and cybersecurity professionals in formulating informed strategies that ensure a Cyber Ready Rural future.

Image-Based PDF Malware Detection Using Pre-Trainned Deep Neural Networks

Tyle Nichols (Texas A&M University); Jack Zemlanicky (Quinnipiac University); Zhirui Luo (New Mexico Institute of Mining and Technology); Qingqing Li (Towson University); Jun Zheng (New Mexico Institute of Mining and Technology)*

jun.zheng@nmt.edu

PDF is a popular document file format with a flexible file structure that can embed diverse types of content, including images and JavaScript code. However, these features make it a favored vehicle for malware attackers. In this paper, we propose an image-based PDF malware detection method that utilizes pre-trained deep neural networks (DNNs). Specifically, we convert PDF files into fixed-size grayscale images using an image visualization technique. These images are then fed into pre-trained DNN models to classify them as benign or malicious. We investigated four classical pre-trained DNN models in our study. We evaluated the performance of the proposed method using the publicly available Contagio PDF malware dataset. Our results demonstrate that MobileNetv3 achieves the best detection performance with an accuracy of 0.9969 and exhibits low computational complexity, making it a promising solution for image-based PDF malware detection.

Text Encryption Using Audio with Multiple Chaotic Maps

Aayushman Singh (Center for Cyber Security Systems and Networks, Amrita Vishwa Vidyapeetham)*; Kurunandan Jain (Center for Cyber Security Systems and Networks, Amrita Vishwa Vidyapeetham)

am.sc.u4cys23002@am.students.amrita.edu

Text encryption serves as a cornerstone in safeguarding confidential information within communication and storage infrastructures. In this paper, we propose an innovative encryption technique employing chaotic systems, notably the 2D Baker's map and the 2D logistic map, renowned for their inherent unpredictability and sensitivity to initial conditions. Our approach integrates audio signals to parameterize these chaotic systems, enhancing encryption robustness and cryptographic strength. Through meticulous experimentation and analysis, we validate the efficacy and efficiency of our proposed methodology. This research not only contributes to the advancement of secure communication protocols but also underscores the potential for integrating chaotic systems with audio signals in enhancing data protection methodologies.
Paper ID 106

EXAMINATION OF ARTIFICIAL INTELLIGENCE INTEGRATION AND ITS IMPACT IN HIGHER EDUCATION

Hala Strohmier (University of South Carolina)*

hala.strohmier@usca.edu

This paper comprehensively investigates utilizing Machine Learning (ML) and Artificial Intelligence (AI) within academic settings. Drawing upon scholarly sources, we explore the strategic deployment of ML algorithms for tasks such as detecting AI-generated content, evaluating students’ graduation potential, and enhancing personalized learning experiences. Our methodology encompasses several key stages, including gathering information about ML, selecting appropriate models, collecting and preprocessing data, model training, evaluation, testing, and comparative analysis. Through rigorous evaluation using diverse datasets, we assess the performance of Decision Trees, Multinomial Naive Bayes, and Neural Network models in accurately classifying text samples. The findings from this study provide valuable insights into the efficacy of ML algorithms in academic contexts and offer practical implications for their implementation.

Paper ID 107

COGNITIVE MODELLING OF BANKRUPTCY RISK: A COMPARATIVE ANALYSIS OF MACHINE LEARNING MODELS TO PREDICT THE BANKRUPTCY

Mahadi Hasan (Emory Healthcare)*; Musfika Jannat Mamata (University of Dhaka); Jahirul Islam (University of South Dakota); Sabuj Saha (Oklahoma state University); Alvi Mahmud (Oklahoma state University)

mahadi.hasan.eswu@gmail.com

Machine learning models can assess the financial health of companies and predict the likelihood of them going bankrupt. Early detection gives companies and stakeholders more time to implement strategies to mitigate financial risks or take corrective actions to avoid bankruptcy. This can be particularly useful for companies as it helps them avoid potential financial difficulties, for example, the recent bankruptcy of Silicon Valley Bank (SVB) has led to market volatility, liquidity disruption, and economic instability. This paper compares machine learning models to determine which model predicts bankruptcy better. The dataset of 20 years of US company bankruptcy was obtained from Kaggle.com and consists of 78682 instances and 21 attributes. In this study, we applied robust preprocessing to increase the accuracy of bankruptcy prediction. It aids in determining significant factors contributing to operation uncertainty and helps regulators and investors forecast the probability of default for better risk management. We applied an 80:20 split for training and validation respectively in our dataset and followed proper tuning of parameters using cross-validation in the training set. We compared several performance matrices, including accuracy and ROC-AUC in various machine learning models such as logistic regression, KNN, decision tree, support vector machine, neural network, and random forest to demonstrate the validity of our study findings. The KNN Classifier has come up champion model with an accuracy of 94.41% and an ROC AUC of 80.45% among all machine learning models as better predictors for bankruptcy.

Paper ID 108

EVALUATION AND ANALYSIS OF A DIGITAL FORENSIC READINESS FRAMEWORK FOR THE IIoT

Sri Harsha Mekala (Deakin University)*; Zubair Baig (Deakin University); Adnan Anwar (Deakin University); Naeem Firdous Syed (Deakin University)

shmek@deakin.edu.au

Digital Forensic Readiness (DFR) is a significant need to facilitate effective incident response in Industrial Internet of Things (IIoT) networks. However, existing frameworks often lack specificity for IIoT environments. In this paper, we develop and implement a criteria for evaluation of a novel DFR framework for the IIoT. We evaluate its effectiveness by aligning it with ISO/IEC 27043:2015 standard, chosen for its broad applicability across a wide range of technologies and its focus on readiness process groups. Our evaluation correlates the framework's stages of operation with standard
processes and contextualizes it with a Modbus TCP attack scenario. This research bridges the gap in IIoT cybersecurity, highlighting the framework's strengths and paving the way for proactive incident detection and improved forensic reporting in dynamic IIoT landscapes.

**Paper ID 109**

**A FRAMEWORK FOR INTEGRATED DIGITAL FORENSIC INVESTIGATION EMPLOYING AUTOGEN AI AGENTS**

Akila Shamendra Wickramasekara (UCD School of Computer Science); Mark Scanlon (University College Dublin)*

mark.scanlon@ucd.ie

The increasing frequency and rapidity of criminal activities require faster digital forensic (DF) investigations. Currently, most DF phases involve manual procedures, requiring significant human effort and time, often facing evolving requirements. This paper proposes an integrated framework employing AutoGen Artificial Intelligence (AI) agents and Large Language Models (LLMs) such as LLAMA, and StarCoder. The suggested framework utilizes AI agents and LLMs to perform tasks articulated in natural language by a human agent. The proposed architecture presents a significant advantage by alleviating the investigative workload and shortening the learning curve for investigators. However, it is still combined with risks such as information accuracy, hallucination impact, and legal barriers. Although, this research contributes to the ongoing discourse on optimizing DF processes in response to the evolving landscape of criminal activities and the corresponding demands placed on investigative resources.

**Paper ID 110**

**BOOSTING AIRCRAFT MONITORING AND SECURITY THROUGH GROUND SURVEILLANCE OPTIMIZATION WITH YOLOv9**

Murat Bakirci (Tarsus University)*; Irem Bayraktar (Tarsus University)

muratbakirci@tarsus.edu.tr

The integration of object detection algorithms into aircraft tracking and ground surveillance systems presents a myriad of security advantages, bolstering the protection of critical infrastructure. These algorithms are instrumental in enforcing access control measures by continuously monitoring and discerning between authorized and unauthorized access to parked aircraft. With ongoing refinements, they serve as crucial components of intrusion detection systems, promptly alerting security personnel to any suspicious or unauthorized activities in the vicinity of grounded aircraft. Effective training of detection algorithms enhances their analytical capabilities, enabling them to discern between routine operations and security-threatening situations with greater precision. Notably, one of the pivotal applications lies in supporting digital forensic investigations, as these algorithms provide detailed activity logs, facilitating comprehensive post-incident analyses and bolstering forensic efforts to understand security incidents or breaches. In this investigation, we assessed the efficacy of the YOLOv9 detection algorithm in identifying aircraft situated on the ground surface. Furthermore, we highlight the significance of satellite imagery in dataset acquisition for object detection algorithms, particularly emphasizing the role of Low-Earth-Orbit (LEO) satellites in real-time image acquisition. Through this comprehensive analysis, we underscore the pivotal role of YOLOv9 in enhancing security measures and compliance with aviation security standards and regulations, ultimately fortifying the security posture within aviation environments.

**Paper ID 111**

**YOLOV9-ENABLED VEHICLE DETECTION FOR URBAN SECURITY AND FORENSICS APPLICATIONS**

Murat Bakirci (Tarsus University)*; Irem Bayraktar (Tarsus University)

muratbakirci@tarsus.edu.tr

The integration of artificial intelligence (AI) techniques in vehicle detection holds significant promise, particularly in forensic and security domains. Leveraging object detection algorithms enables real-time monitoring of vehicles by
competent authorities, aiding in continuous surveillance of roads and highways for various surveillance objectives. Additionally, it streamlines tasks such as identifying stolen vehicles, tracking suspects, and enforcing traffic regulations. Object detection technology also proves invaluable in forensic analysis, aiding criminal investigations and accident reconstructions. Furthermore, it enhances security by detecting aberrant behavior and potential threats at critical infrastructure sites. Concurrently, the remarkable advancements in unmanned aerial vehicles (UAVs) have led to their widespread application across diverse domains, including traffic monitoring and intelligent transportation systems. Equipped with high-resolution cameras, UAVs offer precise imagery for vehicle detection, facilitating swift responses to incidents. This study focuses on vehicle detection from aerial urban transportation images using YOLOv9 on a UAV platform, demonstrating the feasibility and efficacy of aerial analysis for efficient vehicle detection and timely alerts to competent authorities.

**Paper ID 113**

**ENHANCING FORENSIC ANALYSIS WITH AUTONOMOUS UAV DEPLOYMENT FOR AERIAL INVESTIGATION**

Murat Bakirci (Tarsus University)*; Muhammed Miran Özer (Tarsus University)

muratbakirci@tarsus.edu.tr

UAV-based atmospheric measurement systems are an important area of research for forensic investigations, indicating that this technology can increase the potential for environmental justice and public health. This study examines the potential of unmanned aerial vehicles (UAVs) supported atmospheric measurement systems for the use of air quality data in forensic investigations and demonstrates their contribution to the understanding of environmental incidents. The detailed atmospheric data provided by UAVs offers a unique perspective on understanding the causes and impacts of environmental incidents, enabling more precise reconstruction of the chronology of events in forensic processes. The salient results of the study indicate that UAV-based atmospheric measurement systems allow for a more effective analysis of environmental events in forensic investigations. The integration of these technological advances into forensic processes makes a significant contribution to strengthening environmental justice and addressing environmental threats to public health more effectively. This study highlights a unique perspective on how the atmospheric measurement capabilities of UAVs can be used in forensic investigations. The findings highlight how this technological approach contributes to a better understanding of environmental phenomena and a stronger basis for forensic processes.

**Paper ID 114**

**MALWARE API CALL-BASED MULTICLASS-CLASSIFICATION USING MACHINE LEARNING AND DEEP LEARNING**

Sarah Adair (Sam Houston State University)*; Cihan Varol (Sam Houston State University); Fan Liang (Sam Houston State University); Van Vung Pham (Sam Houston State University)

sadair@shsu.edu

Malicious attacks have been on the rise with the growth of technological innovations. With the increase in malicious attacks, many current defense systems focus on preventive and reactive measures. However, the Intrusion prevention system and Intrusion Detection system may not be able to detect all suspicious processes and files that come through the network. Even if the security system detects suspicious activity, it may be unable to quickly classify the type of malware to implement effective and efficient protection. Thus, much research has focused on creating machine-learning models to classify suspicious programs as malicious or benign. However, the limitation of classifying a suspicious file as benign or malicious still does not aid the system in deploying effective security measures to counteract the damage of executed suspicious files. We proposed to train machine learning models and deep learning models to classify the eight most common malware classes. Trained models that can classify malware classes will boost a system’s efficiency in identifying the type of malware, focusing on the affected area, and deploying effective countermeasures to minimize damages. Our experiment shows that the XGBoost model performs the best for tabular data types with an average accuracy of 65%, and the Transformer model achieves the highest accuracy score of 57% for sequential datasets.
A COMPARISON BETWEEN TRANSFORMERS AND FOUNDATION MODELS IN SENTIMENT ANALYSIS OF STUDENT EVALUATION OF TEACHING

Inés Micaela Vega (Universidad San Francisco de Quito); José Valencia (Universidad San Francisco de Quito); Ángel Arcos (Universidad San Francisco de Quito); Danny Navarrete (Universidad San Francisco de Quito); Maria Baldeon Calisto (Universidad San Francisco de Quito)

mbaldeonc@usfq.edu.ec

Student evaluation of teaching (SET) serves as a crucial tool for improving educational quality, enabling students to articulate their opinions about instructors. However, manually evaluating student feedback is time-consuming, subjective, and prone to error. Sentiment analysis, which automatically classifies texts using computational algorithms, presents a promising alternative for this task. In this work, we conduct a comparative analysis of sentiment analysis on SET between three Transformer networks and three Foundation models on a dataset from an Ecuadorian university. Our experiments demonstrate that Transformer models trained on the dataset of interest have a better overall performance than general-purpose Foundation models. Furthermore, among the models examined, DistilBERT emerges as the top performer, achieving an accuracy of 84.90% and an F-1 score of 0.836. In comparison, among the Foundation models, Google Bard achieves the highest accuracy and F-1 score with 78.3% and 0.767, respectively. This work contributes valuable insights to the realm of higher education evaluation, showcasing the potential of advanced NLP techniques to expedite and enhance the SET process, ultimately paving the way for continuous improvement in educational settings.

PERSISTENCE TECHNIQUES IN MICROSOFT ACTIVE DIRECTORY: DETECTION AND MITIGATION STRATEGIES

Zeynep Senturk (Gazi University)*; Erdal Irmak (Gazi University)
zeynep.senturk1@gazi.edu.tr

Microsoft Active Directory Domain Service (ADDS) is one of the key components of information technology (IT) for organizations due to its popularity, underscored by its diverse and easy to use features. The system plays a pivotal role in centralizing network management, facilitating user authentication, and simplifying access control, making it an indispensable tool for seamless and efficient IT infrastructure operations. On the other hand, the service is targeted by attackers quite often due to the same popularity and added criticality. This research explores the Kerberos authentication protocol employed in certain attacks, examines the methods utilized for achieving persistence in Microsoft AD services (Diamond Ticket, Golden Ticket, Silver Ticket, Skeleton Key, and AdminSDHolder), and presents various approaches for detecting and mitigating these security threats. Additionally, an experimental environment has been created to exhibit sample applications of the attacks. Detecting and stopping attacks or persistent operations post-privilege escalation poses a formidable challenge. The focal point of ensuring IT system security lies in preventing attackers during the initial phases of an attack. This resource serves as a valuable repository of information for individuals with IT security tasks within organizations employing the Microsoft AD Service.

THE RELIABILITY OF DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS AND THE POTENTIAL UTILIZATION OF ARTIFICIAL INTELLIGENCE IN THE EVIDENCE EVALUATION PROCESS

Sefa Ata (Hacettepe University)*; Çetin Arslan (Council of Judges and Prosecutors)
sefaata@hacettepe.edu.tr

The digitization process involves transforming all aspects of social life. As a result of this transformation, daily routines have become impossible to carry out without digital capabilities. The impact of digitization also transforms the nature of actions in the context of criminal law. This transformation has increasingly popularized the use of digital evidence
in criminal proceedings. However, due to the unique characteristics of such evidence, its reliability is a subject of debate. This study provides a brief overview of the digitization process and the concept of digital evidence. Subsequently, the reliability issues of digital evidence will be discussed, followed by an exploration of the potential uses of AI-based systems in the evaluation process of digital evidence, considering both the positive and negative aspects.

**Paper ID 118**

**MULTI-TENANT CLOUD SECURITY RISK PREDICTION THROUGH CYBER-VALUE-AT-RISK (CVaR)**

Prashant Vajpayee (UNT)*; Gahangir Hossain (University of North Texas)

prashantvajpayee@my.unt.edu

Cloud computing is a rapidly growing field in information science that has the potential to revolutionize the way we use the Internet. Despite its many benefits, users are often hesitant to store their data in the cloud due to concerns about security, particularly in multi-tenant environments where multiple users share the same resources. To address this challenge, traditional access controls have been implemented in the cloud to ensure the security of the multi-tenant environment. However, these access controls alone are not sufficient to achieve the desired level of security due to the dynamic nature of the cloud environment. The paper discusses about how a weak Authentication, Authorization, and Accounting (AAA) can violate the confidentiality, integrity, and availability (CIA) in cybersecurity. Further, it proposes a risk bases authentication (RBA) approach using supervised learning and calculating risk probability using logistics regression to enable controlled authentication process to secure assets in the multi-tenant cloud environments. The paper explained a method to calculate cyber-value-at-risk (CVaR) using RBA method, access control cost, risk probability, and, asset value. It further utilized financial historic simulation method to elaborate the generation of aggregated CVaR for overall cloud assets in an organizational setting. In summary, cloud computing is a promising technology that can transform the way we use the Internet. However, security concerns remain a major obstacle to its widespread adoption. By integrating AI with RBA, we can enhance the security of multi-tenant cloud environments and protect user data from cyber threats. The proposed CVaR model provides a useful tool for calculating the risk associated with cloud computing and can be used to guide future research in this area.

**Paper ID 119**

**CATCH’EM ALL: CLASSIFICATION OF RARE, PROMINENT, AND NOVEL MALWARE FAMILIES**

Maksim E Eren (Los Alamos National Laboratory)*; Ryan Barron (Los Alamos National Laboratory); Manish Bhattachar (Los Alamos National Lab); Selma Wann (Los Alamos National Laboratory); Nicholas Solovyev (LANL); Kim Rasmussen (Los Alamos National Laboratory); Boian Alexandr (LANL); Charles Nicholas (University of Maryland, Baltimore County)

maksim@lanl.gov

National security is threatened by malware, which remains one of the most dangerous and costly cyber threats. As of last year, researchers reported 1.3 billion known malware specimens, motivating the use of data-driven machine learning (ML) methods for analysis. However, shortcomings in existing ML approaches hinder their mass adoption. These challenges include detection of novel malware and the ability to perform malware classification in the face of class imbalance: a situation where malware families are not equally represented in the data. Our work addresses these shortcomings with MalwareDNA: an advanced dimensionality reduction and feature extraction framework. We demonstrate stable task performance under class imbalance for the following tasks: malware family classification and novel malware detection with a trade-off in increased abstention or reject-option rate.

**Paper ID 120**

**EFFECT OF SIGNAL CONDITIONING AND EVOKED POTENTIAL BASED REPRESENTATION ON STABILITY AND DISTINCTIVENESS OF EEG BRAIN SIGNATURES**

Muhammed E Oztemel (Louisiana State University)*; Omer Soysal (Southeastern Louisiana University)

moztem2@lsu.edu

29
Biometric patterns have been used for authentication purposes for more than decades. Although traditional biometric measurements including fingerprints, facial recognition, and sound recognition are often used for authentication purposes, there is ongoing concern about the risks associated with their repeatability and susceptibility to theft. The utilization of electroencephalography (EEG) has promising potential thanks to the distinctive patterns extracted from brain signals. The main goal of this study is to explore the effectiveness of signal conditioning and evoked potentials on uniqueness and permanence of individuals’ EEG signals for authentication purpose. We utilized the Laplacian of Gaussian as a signal conditioning operator. In addition, three signifying functions were explored in obtaining evoked potential time-domain representation from an individual EEG signal. Different stimuli protocols were employed for comparison. A time-series and a statistical technique were utilized for uniqueness and permanence analysis.

**Paper ID 123**

**ASSESSING THE INTEGRITY OF MOBILE PLATFORM-BASED SENSOR DATA PIPELINES**

Jordan Shropshire (University of South Alabama)*; Jeffrey T McDonald (University of South Alabama)

jshropshire@southalabama.edu

This paper describes the development and evaluation of a framework for assessing the integrity of sensor data flows within mobile sensor-reliant systems such as UAVs, robots, and autonomous vehicles. These platforms rely on internal pipelines for collecting, processing, and distributing sensor inputs to their command and control components. If the integrity of this sensor data feed is compromised then the platform could pose a safety risk. Hence, the new framework is designed to be integrated into the platform so it can detect compromised sensor data pipelines. It ingests raw data directly from sensor input groups and predicts the corresponding values which should emerge from the pipeline under normal conditions. It uses multi-output prediction models for prediction. Predicted and actual output value are compared to determine if the data pipeline has been compromised. If properly integrated, this framework could increase cyber-physical system resilience.

**Paper ID 126**

**THE DEVELOPMENT OF A DIGITAL FORENSIC FRAMEWORK FOR EASE OF FORENSIC ANALYSIS**

Mahika Gupta (PES University)*; Dhruv Suvarna (PES University); Mahesh KM (PES University); Sonal Gabhuri (PES University); Prasad B Honnavalli (PES University); Dr. Sapna V V M (PESU)

pes1ug20cs243@pesu.pes.edu

With the growing use of digital devices and technologies, the volume of digital forensic evidence in need of analysis also increases. This results in a need for more effective methods to conduct analysis of this evidence in an investigation. This project aims to develop a framework for a digital forensic process. The framework will utilize various tools and techniques to enhance the process of collecting, analyzing, and preserving digital evidence. A survey of existing digital forensic tools, including FTK Imager, Autopsy, and The Sleuth Kit was conducted to help identify various pain points faced by investigators throughout the forensic lifecycle. Based on this study, a framework for the analysis of storage data and memory dumps in digital forensics is proposed, incorporating industry best practices and tools such as The Sleuth Kit and Volatility, enhancing ease of use, and thereby promoting more accurate resolutions.

**Paper ID 127**

**FORTT-GEN: NETWORK TRAFFIC GENERATOR FOR MALWARE FORENSICS ANALYSIS TRAINING**

Jonas V Bistene (Military Institute of Engineering)*

jonas.bistene@ime.eb.br

The generation and replication of network traffic are essential tasks for testing, analyzing, simulating, and evaluating the behavior and efficiency of systems, protocols, applications, and network services. However, it faces various challenges and limitations when generating or replicating network traffic in a realistic, responsive, and scalable manner, using appropriate models. This work proposes a modeling of a program for generating and replicating network traffic, called Forensic Training Traffic Generator (ForTT-Gen), aims to address the challenge associated with generating and
replicating network traffic generated by malware by creating files that can be used in the analysis of network packets inherent to forensic analysts’ training. ForTT-Gen is a tool that can generate and replicate network traffic using a hybrid model that combines the replication of real data and the generation of synthetic data through statistical techniques. Experimental results demonstrate the model's ability to reliably. Accurately reproducing the statistical patterns of the original traffic, is evidenced by a determination coefficient of 1 and a Pearson coefficient of 0.9, all within a 0.58 confidence interval with 95% certainty.

Paper ID 128

ANTI-FORENSICS UNDER SCRUTINY: ASSESSING THE EFFECTIVENESS OF DIGITAL OBFUSCATION IN THE CLOUD

Christopher Lowetz (Johns Hopkins University); Grant Shepard (Johns Hopkins University); Joel Coffman (United States Air Force Academy)*

joel.coffman@acm.org

Digital forensics investigations are complicated by anti-forensics techniques that seek to deny or disrupt investigators’ ability to process and analyze evidence. Little extant research describes strategies to detect and defeat attempts to evade investigations of cloud resources. Thus, anti-forensics techniques pose a challenge to cloud investigations, which are already complicated by distributed computing systems that offer seemingly limitless ephemeral storage and few, if any, opportunities for physical access by investigators. To spur further research in this field, we offer a data set with virtual machine (VM) images that include anti-forensic techniques. We provisioned VMs using a popular cloud environment; populated them with user activity; and applied various techniques to destroy, disrupt, and obfuscate the activity patterns. We then obtained evidence in a common forensics format. To demonstrate the utility of our data set, we analyzed our images to determine what activity could be reconstructed in spite of anti-forensics efforts. Many anti-forensic techniques make data recovery either highly unlikely or impossible.

Paper ID 129

ORAT - AN OPEN REDIRECT ANALYSIS TOOL

José Martinho (Instituto Politécnico de Viana do Castelo)*; Diogo Mendes (Instituto Politécnico de Viana do Castelo); Pedro Pinto (Instituto Politécnico de Viana do Castelo)

josemartinho@ipvc.pt

Securing web applications against open redirect vulnerabilities is important for protecting users from malicious redirection and phishing attacks. Open Redirect attacks occur when a malicious actor manipulates a link on a vulnerable website to redirect users to a malicious destination, often disguised as legitimate.

This paper proposes a Google Chrome extension named Open Redirect Analysis Tool (ORAT), a tool that analyses a website for potential open redirect attacks. ORAT enables the detection of such vulnerabilities directly within the browser. It uses a straightforward interface and it simplifies the process of scanning web applications for unsafe redirects by applying a curated set of test payloads to uncover vulnerabilities, from the obvious to the subtle ones.

The tests show that ORAT can identify and present open redirect vulnerabilities. Also, a discussion is provided about the limitations encountered, such as the scope of testing payloads and browser specificity, and a roadmap for future iterations of the proposed tool is proposed. By advancing the capabilities for early detection of redirect vulnerabilities, ORAT contributes to the set of tools available to cybersecurity practitioners and web developers, aiming to foster a secure online environment.
Paper ID 130

EFFICIENT PROGRAMABLE ARCHITECTURE FOR LWC NIST FIPS STANDARD ASCON

Islam A Elsadek (The Ohio State University)*; Islam Tawfil (The Ohio State University)
elsadek.2@osu.edu

NIST finalized the LWC standardization process initiated in 2018 by selecting ASCON as the new standard. ASCON is an AEAD cryptography algorithm featuring three variants “ASCON-128, ASCON-128a, ASCON-80pq” vary in terms of input block size and the number of rounds, etc. In this work an efficient programable hardware design that supports all the three AEAD variants is proposed and implemented over GF22nm, SKY130nm ASIC technologies and Spartan-7 FPGA. The programable design is compared to the HW of each individual variant showing the savings in utilizing the programable design which eliminates the need for three separate standalone designs. Results are shown in terms of area, throughput and Energy efficiency. Results show that the programable ASCON saves 61% of total silicon area. The programable HW has an average energy efficiency overhead of 4% compared to dedicated HW design for each variant. In addition to assessing the programable design, comprehensive study and comparison of the hardware for the individual variants is conducted. ASCON-128a variant is the most energy efficient “2981 Gbits/J” variant with highest throughput “12.16 Mbits/clk”. However, ASCON-128 has the smallest silicon area “2206 μm2”.

Paper ID 131

DYNAMIC CALCULATION OF PASSWORD SALTS FOR IMPROVED RESILIENCE TOWARDS PASSWORD CRACKING ALGORITHMS

Oluwasola Mary Adedayo (The University of Winnipeg)*; Arun Mani (The University of Winnipeg)

m.adelayo@uwinnipeg.ca

Passwords have been an integral part of our lives from the dawn of the internet and keeping them secure has been of paramount importance. Each attempt to secure our digital lives has been met with increased complexity and scope in attacks to compromise security measures. This paper explores a novel methodology to calculate password salts by using the password itself and multiple texts to generate lookup values into a text corpus that is then used to calculate salt values dynamically and on the fly. The proposed method allows an authentication system to use salts for password storage without storing the salts in a database where they might be compromised.

Paper ID 132

DECODING DOOH VIEWABILITY USING YOLO FOR PRIVACY-FRIENDLY HUMAN SILHOUETTE IDENTIFICATION ON LiDAR POINT CLOUDS

Anna Forster (University of Camerino)*; Carlo Lucheroni (University of Camerino); Stefan Gürtler (University of Applied Sciences Northwestern Switzerland)

anna.forster@unicam.it

Traditional methods for measuring digital out-of-home (DOOH) advertising effectiveness often rely on static data or camera footage, leading to limitations in accuracy and real-time insights. This research proposes a novel approach that leverages the combined power of LiDAR technology and YOLOv8, a state-of-the-art object detection model, to achieve precise and privacy-friendly human silhouette identification for DOOH performance measurement. By extracting 3D point cloud data from LiDAR sensors and employing YOLOv8’s efficient object detection capabilities, the model accurately identifies and tracks pedestrians in the vicinity of DOOH displays. This information, combined with LiDAR’s performance under varying weather and lighting conditions, offers a significant improvement over traditional methods, providing advertisers with valuable real-time data on audience engagement and campaign effectiveness. The comparison with the same model performance trained on a standard MC-COCO 2017 dataset presented comparable accuracy but faster inference times. Furthermore, the focus on LiDAR data ensures privacy by avoiding the use of facial recognition or other sensitive personal information. This research demonstrates the feasibility and potential of LiDAR-
based human silhouette identification for DOOH performance measurement, paving the way for a more data-driven and effective advertising landscape.

**Paper ID 133**

**PRIVACY-ENHANCED IMAGE RESTORATION IN REMOTE SENSING VIA FEDERATED LEARNING**

Muhammad Jahanzeb Khan (University of Nevada, Reno)*; Suman Rath (University of Nevada, Reno); Muhammad Hassan Zaib (Air University, Islamabad)

mj25074@gmail.com

This research addresses the dual challenges of image restoration quality and data privacy in optical remote sensing. Traditional restoration methods often fall short due to the complex nature of remote sensing images, and data privacy concerns further complicate the use of advanced techniques. By integrating the Deep Memory Connected Neural Network (DMCN) with the Data-Decoupled Federated Learning (DDFL) framework, our approach enables significant improvements in image restoration without requiring direct access to sensitive raw data. This method not only enhances data privacy by leveraging federated learning principles but also incorporates advanced techniques like Gaussian image denoising to maintain high restoration quality despite potential noise introduced by the federated process. The performance of the federated DMCN, particularly on the UCMERCEd dataset, demonstrates minimal accuracy degradation, even in the presence of noise, while the strategic use of Downsampling Units within DMCN optimizes computational efficiency. Our comprehensive evaluations reveal the effectiveness of this approach in balancing data privacy with the need for high-quality image restoration, suggesting a promising direction for future advancements in remote sensing applications.

**Paper ID 134**

**TOWARDS PRIVACY-PRESERVING VEHICLE DIGITAL FORENSICS: A BLOCKCHAIN APPROACH**

Trent Menard (University of Central Arkansas); Mahmoud Abouyoussef (UCA)*

mahmoud.abouyoussef1@gmail.com

Vehicle digital forensics (VDF), encompasses the investigation of digital evidence related to vehicles, plays a crucial role in modern transportation systems, aiding in accident investigations, crime detection, and ensuring road safety. However, the need to collect data for such investigations has exacerbated privacy concerns, as sensitive vehicular data is susceptible to unauthorized access and exploitation. While blockchain technology has been explored in the literature to address these challenges, existing techniques often prioritize user anonymity over data unlinkability, limiting their effectiveness in preserving privacy. In response, this paper proposes a novel blockchain-based networking strategy for VDF, aiming to achieve both user anonymity and data unlinkability concurrently. By leveraging group signatures and secure communication protocols, the proposed strategy ensures the integrity of vehicular data while mitigating privacy risks. Performance evaluations demonstrate the efficacy of the strategy in terms of computation and communication overheads, while comparative analyses highlight its superiority over existing approaches in terms of privacy preservation and security.

**Paper ID 136**

**CONTRIBUTION OF ALGORITHM VISUALIZATIONS TO STUDENTS’ LEARNING SKILLS: A PEDAGOGICAL APPROACH**

Harem Ali Kheder (Lebanese French University)*; Asaf Varol (The University of Tennessee at Chattanooga)

harem.kheder@lfu.edu.krd

The Domain Algorithm visualizations are multimedia-based representations of algorithms that help students learn how they operate and behave. Algorithm visualizations provide numerous benefits to instructors and students, including an improved understanding of difficult algorithms in programming. By stripping down the complexities of algorithms and presenting them in simplified visual ways, students can obtain a more thorough knowledge of how they perform. Instructional approaches, such as guided instruction or discovery learning, are critical to the pedagogical effectiveness of algorithm representations. Guided instructions can considerably boost learners' overall performance in problem-
solving activities that incorporate visualizations. At the same time, discovery education promotes exploration and experimentation, yet it may result in longer learning times and increased mental demands. A combination of these approaches is required for optimal effectiveness of instruction. In this paper, we investigate how the pedagogical effectiveness of algorithm visualizations should be determined by a variety of elements, including student characteristics, visual and cognitive processing ability, algorithm representation, and instructional context based on a literature review and interviews with field experts, and a bunch of recommendations is provided that has witnessed by authors during their long teaching periods.

**Paper ID 138**

**ALGOXSSF: DETECTION AND ANALYSIS OF CROSS-SITE REQUEST FORGERY (XSRF) AND CROSS-SITE SCRIPTING (XSS) ATTACKS VIA MACHINE LEARNING ALGORITHMS**

Naresh Kshetri (Emporia State University)*; Dilip Kumar (IIT Mandi); James Hutson (Lindenwood University); Navneet Kaur (University of Missouri - Saint Louis); Omar Osama (Binghampton University, SUNY)

NKshetri@emporia.edu

"The global rise of online users and online devices has ultimately given rise to the global internet population apart from several cyberrimes and cyberattacks. The combination of emerging new technology and powerful algorithms (of Artificial Intelligence, Deep Learning, and Machine Learning) is needed to counter defense web security including attacks on several search engines and websites. The unprecedented increase rate of cybercrime and website attacks urged for new technology consideration to protect data and information online. There have been recent and continuous cyberattacks on websites, web domains with ongoing data breaches including - GitHub account hack, data leaks on Twitter, malware in WordPress plugins, vulnerability in Tomcat server to name just a few. We have investigated with an in-depth study apart from the detection and analysis of two major cyberattacks (although there are many more types): cross-site request forgery (XSRF) and cross-site scripting (XSS) attacks. The easy identification of cyber trends and patterns with continuous improvement is possible within the edge of machine learning and AI algorithms. The use of machine learning algorithms would be extremely helpful to counter (apart from detection) the XSRF and XSS attacks. We have developed the algorithm and cyber defense framework - algoXSSF with machine learning algorithms embedded to combat malicious attacks (including Man-in-the-Middle attacks) on websites for detection and analysis."

**Paper ID 141**

**AI BASED GOALKEEPER FOR PENALTY SHOT PREDICTION USING RNN AND PATTERN MATCHING ALGORITHM**

Akshit Naithani (SVKM's NMIMS Shirpur)*; Vrishin Jain (SVKM's NMIMS Shirpur); Tanish Singh Rajpal (SVKM's NMIMS Shirpur); Vansh Mistry (SVKM's NMIMS Shirpur)

naithaniakshit@gmail.com

This paper presents an AI-driven goalkeeper software designed for simulating and predicting penalty shootouts in soccer, utilizing Recurrent Neural Networks (RNN) and pattern matching algorithms. The software aims to enhance victory chances in penalty shootouts by helping in predicting the opposition’s penalty shot direction and allowing real-life goalkeepers to train for it to be ready for match-day scenarios, and also facilitate the training of penalty takers to introduce more randomness in the direction of their shots. It explores the feasibility, technical requirements, and operational aspects of deploying AI goalkeepers, detailing the system architecture, methodology, and implementation. Testing results demonstrate the software's prowess in predicting and saving penalty shots. The paper highlights the significance of AI goalkeeper software in sports training and simulation, suggesting avenues for further efficiency improvements and algorithmic exploration. This research lays the groundwork for AI-driven goalkeeper simulations and their practical usage in sports training, contributing to the advancement of AI-assisted performance analysis in sports.
Paper ID 142

USING ITIL AS PART OF THE NIST CYBERSECURITY FRAMEWORK

Paulo S Teixeira (Polytechnic University of Cavado and Ave)*; Sérgio Lopes (IPCA); Sandro Carvalho (Polytechnic Institute of Cávado and Ave); Patrícia Isabel Sousa Trindade da Leite (Instituto Politécnico Cavado e Ave)

pteixeira@ipca.pt

Modern organizations face increasing challenges in managing IT services while maintaining robust information security. This study explores the potential of combining two established frameworks, ITIL and NIST CSF, to optimize IT service management and strengthen cybersecurity practices.

The analysis commences with an individual examination of the characteristics and benefits of both frameworks. ITIL, a set of best practices for IT service management, and NIST CSF, a cybersecurity framework, offer valuable insights when used independently. However, their combined potential is particularly promising. By employing a methodical approach, we establish a clear correlation between ITIL practices and NIST CSF subcategories, revealing significant similarities and complementary aspects. This analysis highlights how their combined application fosters a more integrated and effective approach to managing IT services and enhancing security.

By leveraging the strengths of both frameworks, organizations can achieve a dual benefit: improved quality and efficiency of IT services, alongside strengthened cyber defenses. This study emphasizes the value of a holistic perspective in IT service management and cybersecurity. It suggests that through the strategic integration of practices from both fields, organizations can achieve sustainable operational excellence and robust protection against cyber threats.

Paper ID 144

INVESTIGATION OF PRE-SERVICE TEACHERS’ DIGITAL WELL-BEING LEVELS WITH RESPECT TO VARIOUS VARIABLES

Ebru Polat (Fırat University); Songül Karabatak (Fırat University)*; Müslim Alanoğlu (Fırat University)

s_halici@hotmail.com

This study aims to investigate the levels of pre-service teachers' digital well-being concerning various variables. The research employed a survey model, which is a quantitative research method. The participants in the study were 309 pre-service teachers enrolled at a university in eastern Turkey. The study utilized a Personal Information Form and the Digital Well-being Scale. The study's findings indicate that the participants' overall digital well-being, digital satisfaction, and digital wellness scores were high, while their safe and responsible behavior scores were moderate. Gender did not emerge as a significant factor in the digital satisfaction and safe and responsible behavior sub-dimensions, but it showed a significant difference in favor of female pre-service teachers in the digital wellness sub-dimension. Moreover, the digital satisfaction sub-dimension showed a notable difference in favor of pre-service teachers who reported Internet usage of more than 5 hours and 3-5 hours. The general Digital Well-Being Scale and its sub-dimensions demonstrated a significant difference in favor of participants who reported updating their mobile device security tools a few times a month.

Paper ID 146

INVESTIGATION OF TEACHERS’ KNOWLEDGE MANAGEMENT AND KNOWLEDGE HIDING BEHAVIORS

Songül Karabatak (Fırat University)*; Müslim Alanoğlu (Tuskish Embassy in Podgorica); Ebru Polat (Mustafa Kemal University)

s_halici@hotmail.com

The aim of this study is to investigate the correlation between teachers' knowledge management and their knowledge hiding behaviors. The sample for this study, which was constructed using the correlational model as one of the
quantitative research approaches, consists of 201 teachers selected through simple random sampling. The findings suggest that teachers demonstrate a moderate level of knowledge management, while their level of knowledge hiding behavior is low. Gender does not have a significant impact on teachers’ knowledge management and knowledge hiding behaviors, although there is a significant difference in knowledge management favoring teachers in special education institution. Additionally, the study reveals a negative and moderately significant correlation between teachers’ knowledge management and knowledge hiding behaviors, and no significant relationship between these variables and seniority is observed.

Paper ID 147

ASSESSING THE HEALTH OF A NETWORK UNDER ATTACK

Pedro Marques (British Telecom)*; Alfie Beard (British Telecom); Jonathan Francis Roscoe (BT)

pedro.dm.marques@gmail.com

When faced with a malware outbreak, the health of a computer network is hard to quantify. Calculating the number of infected nodes is a straightforward approach, but it fails to capture intricacies of the devices that make up the network. The choice between which of two network states is preferable might not correlate directly with the number of infected nodes in each, as different nodes carry different importance to the overall function of the network. In this paper we propose a method of assessing the health of a network under attack from a malware outbreak. The proposed method allows for a quantitative measure of how well a network is handling a malware outbreak, as well as the comparison between different network states and the ranking of possible mitigating actions. The method proposed can be adapted to different networks, with its usefulness increasing with the amount of data available for a given network.

Paper ID 148

TOWARDS NEXT-GENERATION SMART SANDBOXES: COMPREHENSIVE APPROACH TO MOBILE APPLICATION SECURITY

Ezgi Gücüyener (Yıldız Technical University)*; Mehmet Amaç Güvensan (Yıldız Technical University)

ezgi.gucuyener@std.yildiz.edu.tr

Sandboxing has been a common practice to isolate apps from each other and protect the overall system from malicious software. With the proliferation and increased accessibility of mobile devices, mobile malware has become more insidious and erratic. Thus, sandboxes are facing the threat of being less effective at detecting malware. This paper has the aim of describing the evolution of mobile sandboxes and proposing an improved approach for advanced sandbox architecture to decrease the possibility of sandbox evasion. Building smart sandboxes is becoming indisputably important for mobile security. Today, mobile malware can perform malicious activities rather easily since sandboxes are not good enough to mimic the behaviour of a real user mobile device. Therefore, detecting malware to halt it's malicious activities is hard but important to protect mobile devices. However, building a smart sandbox environment which behaves as if it were a real user device to trick malware is more valuable based on logic of zero-trust. Two notable challenges have been considered in this study.recognition of typical sandbox environments and evasion techniques adopted by malware through the detection of lack of user activities within sandboxes. This study examines current mobile sandboxing techniques, specifies the requirements to propose a trustworthy mobile sandbox methodology which deals with lack of real user behavior and overcomes the risk of sandbox evasion. With proposed smart sandbox architecture, environmental awareness of malware would be reduced and defense against advanced mobile malware attacks will be strengthened.

Paper ID 149

FRAMEWORK FOR EARLY CYBER ATTACK DETECTION USING ML MODELS DEPLOYED ON FOG DEVICES

Uday Aditya Kasturi (PES University)*; Prateek N Kamath (PES University); Yuktha Poral (PES University (PESU) ); Baddela Divya Malika (PES University); Vadiraja Acharya (PES University)
The growing Internet of Things (IoT) is set to link facets of life including intelligent structures, residences, and whole urban areas. A key factor propelling this growth originates from progress, in the semiconductor sector. IoT promises innovative services demanding extensive data centers and real-time processing capabilities. However, an advancement in technology also promises an advancement in the attack surface and the threats these devices will have to face.

IoT security is an up-and-coming field, raising awareness of the need for security mechanisms for these constrained devices. Existing solutions are computationally heavy for a traditional constrained device in the Fog. With the limitless implementations of these devices, there is a need for a security solution that can be scaled to a large majority of IoT applications.

This paper presents a Python-based Framework with a variety of security methods and functions aimed at the early detection of Cyber Attacks using multiple ML models in real-time. The Framework is tested on a Raspberry Pi 4 device deployed within the fog computation layer, functioning as an intermediary between edge and cloud layers. This fog device is subsequently linked to a network of IoT devices. A distinctive aspect of this Framework is its dual perspective, catering to both developers and general users.

**Paper ID 150**

**IMAGE FORGERY DETECTION USING CONVOLUTIONAL NEURAL NETWORKS**

Ayesh Buddhima Meepaganithage (University of Nevada Reno)*; Suman Rath (University of Nevada, Reno); Mireea Nicolescu (University of Nevada, Reno); Monica Nicolescu (University of Nevada, Reno); Shamik Sengupta (Department of Computer Science & Engineering, University of Nevada)

ayesh@nevada.unr.edu

With the advancement of technology, the ability to forge realistic images has become increasingly accessible, and this has led to a significant challenge in the digital forensics field. A lot of research has been conducted in this area to address this challenge. Traditional image forgery detection methods are time-consuming and slow. Therefore, deep learning methods have played a vital role in image forgery detection. In this research, we investigate the use of convolutional neural network models for image forgery detection and evaluate their performance. From the experimental results, it can be seen that ResNet models have demonstrated high performance in detecting forged images accurately. Out of all the convolutional models we evaluated, the ResNet-101 model obtained the best results, with 93.46% accuracy, 95.08% precision, 92.10% recall, 94.91% specificity, and 93.57% F1-score. ResNet-101 model correctly identified 621 out of 650 authentic images and 584 out of 650 forged images.

**Paper ID 152**

**CYBER-SECURITY KNOWLEDGE GRAPH GENERATION BY HIERARCHICAL NONNEGATIVE MATRIX FACTORIZATION**

Ryan C Barron (UMBC)*; Maksim E Eren (Los Alamos National Laboratory); Manish Bhattacharai (Los Alamos National Lab); Selma Wanna (LANL); Nicholas Solovyev (LANL); Kim Rasmussen (LANL); Boian Alexandrov (LANL); Charles Nicholas (University of Maryland, Baltimore County); Cynthia Matuszek (UMBC)

ryanb4@umbc.edu

Much of human knowledge in cybersecurity is encapsulated within the ever-growing volume of scientific papers. As this textual data continues to expand, the importance of document organization methods becomes increasingly crucial for extracting actionable insights hidden within large text datasets. Knowledge Graphs (KGs) serve as a means to store factual information in a structured manner, providing explicit, interpretable knowledge that includes domain-specific information from the cybersecurity scientific literature. One of the challenges in constructing a KG from scientific literature is the extraction of ontology from unstructured text. In this concept paper, we address this topic and introduce a method for building a multi-modal KG by extracting structured ontology from scientific papers. We demonstrate this concept in the cybersecurity domain. One modality of the KG represents observable information from the papers, such as the categories in which they were published or the authors. The second modality uncovers latent (hidden) patterns of text extracted through hierarchical and semantic non-negative matrix factorization (NMF), such as named entities, topics or clusters, and keywords. We illustrate this concept by consolidating more than 2 million scientific papers
Occupancy grid maps are one of the most robust environment representations to use for problems in robotics such as exploration, navigation, etc. If the partial occupancy maps are used after predicting the uncompleted parts of the map, it is expected that the performance of these tasks will be increased. Therefore, in this paper, we suggest completing partial occupancy maps by using door discovery. In order to do this, initially we find door positions by utilizing geometrical features of the maps and then we implement map completion using image processing techniques based on these door positions. The experimental results show that our approaches are promising with average IoU score up to 0.8790 and have potential to improve the robotic tasks.

Evolutionary analysis of adherence to the ISO 27001:2013 standard in Portugal: Regional and sectoral study

The growing threat of cybercrime and the explosion of data volume raise critical concerns about information security. Organizations must implement systems that manage, ensure the quality, integrity, and security of information. These systems should adhere to the globally recognized ISO 27001:2013 standard. Certification against this standard has become increasingly important in the business world, prompting an examination of Portugal's progress in this area. This study investigates the evolution of the number of ISO 27001:2013 certified companies in Portugal, including a regional and sectoral analysis of information security management system adoption.

Feature selection using Pearson Correlation with Lasso Regression for Intrusion Detection System

The growth of Internet users and traffic drives significant changes in the network security domain. Computer networks become increasingly vulnerable to attack by irresponsible parties, which can potentially cause substantial loss and damage due to information stealing, sending malicious packets, and overtaking network resources. While the effort to secure the network has been conducted persistently, unfortunately, the variety and volume of cyber threats have continuously increased. As such, there is a demand for an effective and efficient attack detection model to prevent this catastrophic network failure by implementing feature selection techniques to reduce the dimension of the feature on a dataset. We proposed a feature selection method combining the Pearson Correlation method with Lasso Regression to address that need. The Pearson Correlation is used to select the best feature based on its degree of relationship. After that, the selected result is optimized using Lasso Regression to achieve the best features for the IDS model. This study reveals that this proposed method significantly improves the SVM classifier's accuracy and false positive rate from 76.45% to 97.17% and 20.67% to 1.44%, respectively.
Paper ID 156

CLOUD COST FACTORS AND AWS COST OPTIMIZATION TECHNIQUES

Ganesh Kumar Murugesan (None)*

ganeshkumarbio@gmail.com

Cost has been a key benefit in migrating the application and data to cloud in addition to the built-in capabilities available. Eventually this key factor which attracts the migration to cloud, has taken a sharp turn and made the enterprises think whether to stay on the cloud or switch back to on-premise or a hybrid setup. This article attempts to identify the external and internal factors and common pitfalls during cloud migration that drive up the cloud cost. Also, various techniques and best practices that are potentially available today to help optimize the higher cost on compute, storage, and data transfer specific to AWS Cloud is being discussed, but similar approach can be implemented with other cloud providers as well.

Paper ID 158

CASSAVA PLANT DISEASE DETECTION USING TRANSFER LEARNING WITH CONVOLUTIONAL NEURAL NETWORKS

Julia Alford (Trinity University); Eva Tuba (Trinity University)*
etuba@ieee.org

Cassava vegetable represents one of the main food sources in some regions like Africa. It can be affected by plant diseases which can increase food insecurity in areas where the plant is relied upon. An early detection, identification and classification of cassava plant disease may be a beneficial tool. Manual field examination can be expensive in many ways, monetary, working time, physically exhausting, etc. Automated detection and identification of plant diseases can be done by analysis of field/plant images. In that case, machine learning can be used to classify the states of these plants. This paper is concerned with building a convolutional neural network (CNN) using transfer learning to create a model for an unbalanced dataset that is more accurate and efficient than existing CNN models. Tested and compared pre-trained models include ResNet101V2, ResNet50V2, EfficientNetB2, VGG16, VGG19, and MobileNet2. After initial testing and results, based on test accuracy, training accuracy, and output trends, further improvements were made by using VGG19. This model was further fine-tuned for the cassava plant disease classification. The resulting model achieved a training accuracy of 99.31% and a test accuracy of 80.27% with the use of 50 epochs which outperforms current results from literature.

Paper ID 159

CREDIBLE DIFFUSION: IMPROVING DIFFUSION MODELS INTERPRETABILITY WITH TRANSFORMER EMBEDDINGS

Matvei Popov (Trinity University); Eva Tuba (Trinity University)*
etuba@ieee.org

This paper introduces a novel approach to enhancing the interpretability and accountability of diffusion models in generative image tasks. By integrating a transformer-based encoder-decoder mechanism, we propose a methodology that employs deterministic degradation operators, derived from dataset labels or associated textual content, as an alternative to traditional random Gaussian noise. This method enables precise attribution of the generated images to their sources within the training data. Through extensive experiments on a subset of the Fashion-MNIST dataset we demonstrate the model's capability to perfectly reconstruct the textual citations while achieving close approximation in image reconstruction. Despite the observed limitations in diversity, our findings indicate a significant potential for
controlled image synthesis based on textual descriptions. This work lays the foundation for advancing the interpretability of generative AI models, paving the way for more transparent and accountable generative applications.

**Paper ID 160**

**OPTIMIZING MACHINE LEARNING FOR BREAST CANCER DETECTION BY HYBRID METAHEURISTIC APPROACH**

Timea Bezdan (Singidunum University); Ivana Strumberger (Singidunum University); Milan Tuba (Singidunum University)*

tuba@ieee.org

Breast cancer ranks as one of the top causes of cancer-related deaths among women worldwide, highlighting the need for improved diagnostic methodologies. Machine learning offers promising solutions; however, the models’ performance highly relies on optimal hyperparameter configurations. The goal of this research is to improve the precision of machine learning models in diagnosing breast cancer by employing a novel optimization strategy that integrates the metaheuristic algorithm, namely, the Sine Cosine Algorithm with the Opposition-Based Learning mechanism for hyperparameter tuning. We applied five machine learning classifiers: K-Nearest Neighbors, Decision Trees, Random Forest, Logistic Regression, and Support Vector Machines to the Breast Cancer Wisconsin dataset. The proposed optimization method was utilized to fine-tune the hyperparameters of these classifiers to improve the performance. Model performance was rigorously evaluated using fivefold cross-validation approach and it was compared to existing methods. The optimization process led to significant improvements in model performance, with the enhanced classifiers outperforming their baseline configurations and existing works. The findings highlight the success of the suggested method in navigating the hyperparameter search space, leading to more accurate and reliable breast cancer diagnoses. Integrating the Sine Cosine Algorithm with Opposition-Based Learning for hyperparameter tuning presents a powerful approach to refining the machine learning classifiers for breast cancer diagnosis. This study underscores the potential of advanced optimization methods in improving the diagnostic capabilities of machine learning models, contributing to timely diagnosis and treatment of breast cancer.

**Paper ID 162**

**LLM-DRIVEN SAT IMPACT ON PHISHING DEFENSE: A CROSS-SECTIONAL ANALYSIS**

Hafzullah İş (Batman University)*

hafzullah.is@batman.edu.tr

Amidst the growing sophistication of phishing threats that exploit human vulnerabilities, this study investigates the effectiveness of Security Awareness Training (SAT) enhanced by Large Language Models (LLMs). Targeting a diverse group of 1,270 participants, including academicians, officers, and students, it aims to evaluate whether LLM-driven SAT can strengthen phishing defenses and cultivate a more resilient digital environment. Initial assessments revealed a baseline Phish Prone Percentage (PPP) of 18.3%, indicating a pronounced vulnerability across participant groups. The deployment of an LLM-enhanced SAT program, characterized by its adaptive and interactive training modules, led to a significant post-training reduction in PPP to 6.3%. This outcome demonstrates the program’s success in mitigating phishing risks and underscores the necessity of evolving SAT strategies to combat the dynamic nature of phishing attacks.

The study’s findings, illustrating a substantial improvement in phishing defense capabilities through LLM-integrated SAT, advocate for the integration of advanced technologies in cybersecurity education. By effectively lowering phishing vulnerability from 18.3% to 6.3%, this research highlights the critical role of innovative training methodologies in enhancing digital security across varied academic and professional landscapes.

**Paper ID 164**

**ADVANCEMENTS IN OBJECT DETECTION FOR UNMANNED AERIAL VEHICLES: APPLICATIONS, CHALLENGES, AND FUTURE PERSPECTIVES**
Anıl Sezgin (National Defence University)*; Aytug BOYACI (Turkish Air Force Academy, National Defence University)
anilszgn@gmail.com

Unmanned Aerial Vehicles (UAVs) are used in different fields ranging from recreational vehicles to agriculture, environmental monitoring, infrastructure inspection, disaster management, security, surveillance and logistics. This paper provides an overview of UAV applications and highlights the importance of object detection in improving drone autonomy. Object detection facilitates tasks such as precision agriculture, disaster response, environmental protection, infrastructure inspection and autonomous navigation. The paper reviews recent advances in UAV-specific object detection algorithms and methodologies and highlights challenges such as varying altitudes, motion blur, real-time processing constraints and limited computational resources. Solutions and adaptations are discussed to overcome these challenges, including lightweight neural network architectures, transfer learning, data augmentation, edge computing, multi-sensor fusion, attention mechanisms and adaptive algorithms. The study highlights the importance of integrating object detection systems into UAVs to improve their use in various sectors and contribute to improvements in surveillance missions.

**Paper ID 165**

**DEEP LEARNING BASED BRAIN TUMOR CLASSIFICATION FOR MR IMAGES USING RESNET50**

Ömer Miraç Kökçam (Fırat University)*; Aytug Boyaci (Turkish Air Force Academy, National Defence University); Muhammed E Çolak (Fırat University)
omkokcam@firat.edu.tr

Brain tumors are abnormal cell growths that occur in various parts of the brain, and the accurate classification of these tumors plays a critical role in determining treatment methods. Advances in medical imaging technologies enable the classification and diagnosis of brain tumors using artificial intelligence and deep learning models. These technologies, assist healthcare professionals to detect tumors in a fast and accurate way, thus increases chance the disease to be diagnosed at early stages and be treated effectively. Concurrently, the development and improvement of artificial intelligence-based classification methods is seen as a very important step in brain tumor diagnosis and treatment. In this study, the ResNet50 model optimized by Google Research and pretrained with ImageNet-21k is used for brain tumor classification. This model is a deep learning-based image classification tool and is capable of learning from large data sets. The model is specifically trained for high-resolution image recognition and is designed to achieve high accuracy rates. The results showed a classification accuracy of 99.9 percent, which is an exceptional accuracy rate for this model. This accuracy rate indicates that the model is highly effective in detecting and classifying brain tumors. High accuracy rates allow for early diagnosis of patients' diseases and, as it is often said in medicine, "Early Diagnosis Saves Lives". This result is one of the many proofs of how effective artificial intelligence and deep learning are in medical image analysis.

**Paper ID 166**

**A REAL-TIME HAND SIGN LANGUAGE RECOGNITION SYSTEM FOR THREATENING SITUATIONS USING DEEP LEARNING**

Zardasht A. A. Shwany (Erbil Polytechnic University)*; shayda khudhur ismaiel (ministry of higher education); karwan hoshyar khalid (EPU); Twana Mustafa (Fırat University); Murat Karabatak (Fırat University); Nashwan Adnan Othman (Knowledge University, Al-Kitab University)
zaraszat.abdulkarim@epu.edu.iq

Hand sign language has been done as physical movements in natural languages that humans have used since ancient times, along with letters, words, and spoken language. This paper presents a real-time method to identify threatening signs by criminals during interrogation, which increases their criminal rank and helps to reach conclusions. The proposed method is to install a camera of appropriate quality in front of the offender, record hand gestures in a specific area of the hand, apply some image processing techniques, such as contrast enhancement techniques, to the image to facilitate recognition as input, and then classify the images using a convolutional neural network (CNN) for a specific problem with high specifications for that topic by and using AlexNet. The accuracy of the presented method is more than 94.2% in real-time testing.
EXAMINATION OF OBJECT TRACKING STUDIES USING DEEP LEARNING: A BIBLIOMETRIC ANALYSIS STUDY

Sevinç AY (Fırat University)*; Songül KARABATAK (Fırat University); Murat Karabatak (Fırat University)
say@firat.edu.tr

The increasing amount of data obtained with advancing technology has led to the growing popularity of deep learning algorithms. Within the scope of this study, the aim was to examine the use of object-tracking algorithms, which are one of the most commonly used areas of deep learning. To contribute to the literature, a bibliometric analysis was conducted. For this purpose, a bibliometric analysis was carried out on 1209 articles accessed through the Web of Science database using the keywords "deep learning" and "object tracking". Vosviewer (version 1.6.20) and R studio Bibliometrix package programs were used for this purpose. In the analysis, it was determined that the highest number of publications was reached in 2022 among the studies conducted between 2012 and 2024. Additionally, it was observed that the majority of the studies were conducted in China, the USA, and South Korea. The prominent keywords in these articles were deep learning, object tracking, object detection, target tracking, and feature extraction, in that order. The research indicates a growing trend in the use of deep learning in the field of object tracking in recent years. Furthermore, it was identified that object detection, which stands out in object tracking studies, is also a popular research topic. It is believed that this study will pave the way for further research in this area.

BIBLIOMETRIC ANALYSIS OF ARTIFICIAL INTELLIGENCE IN UTILIZED DISTANCE EDUCATION AND DISTANCE LEARNING STUDIES

Sevinç Ay (Fırat University)*; Songül KARABATAK (Fırat University); Murat Karabatak (Fırat University)
say@firat.edu.tr

In the contemporary era, wherein artificial intelligence is gaining increasing prominence, its presence and significance are being witnessed in various facets of our daily lives. It is widely believed that artificial intelligence will pave the way for novel advancements in the realm of education, a domain that is profoundly influenced by its influence. Consequently, delving into the ramifications of artificial intelligence on distance education, which has become an integral component of the educational process, assumes paramount importance. This study undertook a comprehensive bibliographic analysis, utilizing data sourced from the Web of Science database encompassing the period between 1993 and 2024, obtained through searches employing the keywords "artificial intelligence" and "distance learning" or "distance education". The findings were assessed based on keywords, authors, documents, sources, and countries. While the keywords were thoughtfully diversified to ensure that studies in this domain were not inadvertently overlooked, the outcomes reveal that there exists ample scope for further research in this field, necessitating the publication of new scientific works.

INVESTIGATION OF EFFICIENCY AND ACCURACY OF DEEP LEARNING MODELS AND FEATURES WITH ELECTROENCEPHALOGRAM (EEG) DATA FOR BINARY CLASSIFICATION

Kelly Obrien (Technological University of Shannon); Liam F Brown (TUS); Joaquim Gonçalves (Polytechnic Institute of Cavado and Ave)*
jgoncalves@ipca.pt

Electroencephalogram (EEG) data is regularly used with Machine Learning to further develop the Medical Technology field. This research investigates the effectiveness of the popular Deep Learning models with a binary classification...
problem with the subjects’ EEG data. The dataset used for this research comprised of EEG data available online that was recorded from human subjects who were labelled as either alcoholic or control. Each subject was presented visual stimuli and brainwave data was recorded through 64 electrodes located on each subject’s scalp. Three types of features were included in this study: Raw signal data, Discrete Wavelet Transform (DWT) and Continuous Wavelet Transform (CWT). The study investigated how several Neural Network models performed when trained with the different features. The models were Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), Gated Recurrent Units (GRU) and Temporal Convolutional Network (TCN). The Convolutional Neural Network performed the best with the highest overall accuracy and the best AUC Score when trained with Raw data and Discrete Wavelet Transform. The Temporal Convolutional Network yielded the best AUC Score when trained with Continuous Wavelet Transform.

**Paper ID 172**

**EXAMINING THE RELATIONSHIP BETWEEN DIGITAL WELL-BEING, DIGITAL HOARDING AND MOBILE INFORMATION SECURITY AWARENESS WITH ASSOCIATION RULE**

Songül Karabatak (Fırat University)*; Müslim Alanoğlu (Tuskish Embassy in Podgorica ); Murat Karabatak (Fırat University)

The aim of this study was to investigate the relationships between digital well-being, digital hoarding, and mobile information security awareness. The study employed data mining methods and was conducted as a correlational study. Data collection involved the use of the Digital Well-Being Scale, Digital Hoarding Scale, and mobile Information Security Awareness Scale. The study utilized data from a total of 466 students enrolled at the Faculty of Education at Fırat University. The collected data underwent preprocessing techniques for data cleaning, transformation, and reduction. Descriptive and correlational analyses were carried out as essential components of the data analysis process. Descriptive analysis included calculating means, percentages, and frequency analyses. For correlational analysis, the association rule was employed to uncover relationships between variables. The results of the study indicated that university students overall exhibited a significant level of digital well-being. However, their awareness of mobile information security and inclination to hoard digital content were considered to be moderate. The findings revealed that individuals who were concerned about file deletion demonstrated considerate behavior towards other users on social media and recognized the impact of digital security on social media interactions.

**Paper ID 173**

**COMPARISON OF IDS IN IOT, MOBILE AND CLOUD BASED SYSTEMS**

Görkem GÖK (Fırat University); Aytug BOYACI (Turkish Air Force Academy, National Defence University); Mustafa Ulas (Fırat University)*

This study is meant to research the evolution of intrusion detection and network monitoring within computer, cloud-based systems, IIoT, and mobile environments. The source has outlined the novel technologies in IDS, from "Fast Learning Network" to hybrid classifiers aiming at protecting cloud computing. The findings highlight innovation IDS technologies that provide flexible and peculiar solutions to ward off potential cyber threats. In addition, it presented with the use of Nagios, NConf, the state of the art in network traffic monitoring, and deep learning as tools for advanced management and network protection. Besides, the research also reviewed concepts of Big Data Analytics and Federated Learning in bettering direct integration and anomaly detection in IIoT. A good comparison of the two would show that recent technological advancements are much needed for network efficiency and its cybersecurity. Based on the findings, the scope of networked system security develops dynamically amid current challenges.

**Paper ID 174**

**CLASSIFICATION OF ECG SIGNALS ENCRYPTED WITH CNN BASED AUTOENCODER WITH LSTM**

Merve Akkuş (Batman University)*; Murat Karabatak (Fırat University); Ramazan Tekin (Batman University)

merve.gtmez@gmail.com
Electrocardiogram (ECG) plays a critical role in the early prevention and diagnosis of cardiovascular diseases. The signals obtained from the electrocardiogram device used in the diagnosis of heart diseases are obtained by healthcare personnel and used to detect arrhythmia. Many cardiac abnormalities show up on an ECG, including arrhythmia, which means an abnormal heart rhythm. The basis of arrhythmia diagnosis is the identification of normal and abnormal heartbeats and their correct classification based on ECG morphology. By compressing ECG signals, Autoencoder can obtain time series signal features and these signals can be used for classification purposes. This work is carried out using a 19-layer network structure that includes a convolutional autoencoder for ECG signal compression and a long short-term memory (LSTM) that processes the encoder output for classification purposes. This structure was used after preprocessing the ECG signals to achieve higher arrhythmia classification accuracy. In the study, the open access MITBIh arrhythmia dataset taken from PhysioNet was used. In the results of the study, when statistical measurements such as precision, accuracy, specificity and sensitivity used to determine the performance of the classification were evaluated, it was seen that it was successful.

**Paper ID 175**

**INVESTIGATION OF TEACHER CANDIDATES' DIGITAL OBESITY**

Sevinç Ay (Fırat University)*; Songül Karabatak (Fırat University); Murat Karabatak (Fırat University)

say@firat.edu.tr

The objective of this study is to investigate the phenomenon of digital obesity among teacher candidates. To achieve this goal, a survey model was employed as a quantitative research method. The participants of this study consisted of 256 teacher candidates who were conveniently sampled from Firat University in Elazığ. To gather relevant information about the teacher candidates, the Digital Obesity Scale was incorporated into the data collection instrument. According to the results obtained from the study, it has been observed that a significant number of teacher candidates use digital devices between 4 and 6 hours per day, and those who use them for more than 7 hours are at a level that needs to be taken into consideration. It has been revealed that teacher candidates mostly use WhatsApp and Instagram. Additionally, it has been revealed that teacher candidates use digital tools mostly for interaction and educational purposes. It has been concluded that the level of digital obesity among teacher candidates is moderate and that gender and the duration of digital device use affect digital obesity to some extent.

**Paper ID 176**

**DISCOVERY OF NEW CHAOTIC SYSTEMS: BASED ON EXISTING SYSTEMS**

Tuncay Cigal (Adıyaman University)*; Erkan Tanyıldızı (Fırat University)

tcigal@adiyaman.edu.tr

Chaotic systems have been an important area of focus for researchers in science and engineering because they reflect the complexity and uncertainty of nature. The discovery of new chaotic systems is an important step towards a better understanding and control of the real world. This work aims to construct new chaotic systems based on existing chaotic systems and makes an important contribution to this field. The developed method has been successfully validated on one-dimensional chaotic systems. Detailed analysis of the generated chaotic systems shows that they effectively fulfill the basic requirements of chaotic properties. These findings suggest that this new approach may have significant potential in many practical applications in the future.