FIRAT UNIVERSITY

IEEE Turkey Section ISDFS'21 International Symposium on Digital Forensics and Security

9th INTERNATIONAL SYMPOSIUM ON DIGITAL FORENSICS AND SECURITY

SYMPOSIUM PROGRAM AND ABSTRACTS

EDITED BY

PROF. DR. ASAF VAROL

ASSOC. PROF. DR. MURAT KARABATAK

ASSOC. PROF. DR. CİHAN VAROL

June 28-29, 2021

Elazığ / Turkey

Consortium Members:

9TH INTERNATIONAL SYMPOSIUM ON DIGITAL FORENSICS AND SECURITY

28-29 JUNE 2021

ELAZIĞ - TURKEY

SYMPOSIUM PROGRAM AND ABSTRACTS

EDITED BY

PROF. DR. ASAF VAROL

ASSOC. PROF. DR. MURAT KARABATAK

ASSOC. PROF. DR. CİHAN VAROL

ELAZIĞ - TURKEY

2021

WELCOME NOTE FROM GENERAL CHAIR

On behalf of the Organizing Committee and Consortium Members of ISDFS, we welcome you to the 9th International Symposium on Digital Forensics and Security (ISDFS 2021) in Elazig, Turkey. Because of COVID-19, last year's ISDFS event was completely held remotely. While we were hoping to have a 100% face-to-face event for this year, due to pandemic situations around the world, we decided to have both in-person and remote attendance for ISDFS 2021.

ISDFS has been always an exciting event as we continue to grow and adapt, motivated and responsive to the technological advances and challenges in the field of Digital Forensics, Cyber Security, Cryptography, and Data Privacy. The world of Cyber Security, as the umbrella terminology, is an exciting area in which to work and study and we'll continue to meet and bring inspired people together in forums like this, to ensure our ISDFS remains at the cutting edge.

ISDFS was originally held in May 2013, at Firat University, Turkey. While this year, we are gathering together remotely and in Elazig, Turkey for the 9th event, previously we also had very successful events at Huntsville-The Woodlands, Texas, USA; Ankara, Turkey; Little Rock, Arkansas, USA; Tirgu Mures, Romania; Antalya, Turkey; and Barcelos, Portugal.

ISDFS is organized by a consortium consists of Maltepe University (TR), Firat University (TR), Sam Houston State University (USA), Gazi University (TR), San Diego State University (USA), Arab Open University (LB), Hacettepe University (TR), Polytechnic Institute of Cavado and Ave (PT), Balıkesir University (TR), Ondokuz Mayis University (TR), Association of Software and Cyber Security of Turkey, Informatics Association of Turkey, Recep Tayyip Erdogan University (TR), Singidunum University (Serbia), TELUQ University (Quebec-Canada), and Yıldız Teknik University (TR).

The symposium's technical program is organized into five tracks; Digital Forensics, Cyber Security, Data Privacy, Cryptography, and Computer Science in general. Moreover, a Special Session on P2834 Standards for Secure and Trusted Learning Systems is part of the event. Two Keynote Speakers are invited to the conference. Dr. Ahmet Koltuksuz will talk about "Cyber Warfare: Changing Doctrines of Warfare, From Sun Tzu to Cyberspace" and Mr. Nicolas Hughes will discuss "A time of reckoning? Changing regulatory and judicial attitudes and the potential impact on digital forensics". In addition, the Informatics Association of Turkey will hold a panel session on Financial Systems, AI, and Cyber Security.

Since 2016, the conference has been sponsored by the IEEE Society and scholarly works disseminated in the symposium have been cited by Xplore Scientific Index. This year, the IEEE Turkey Section sponsored the event technically and the papers presented at the conference will be published again in IEEE Explore.

I would like to express my sincere gratitude and appreciation to all of the consortium members for helping ISDFS to grow each year. We have received 76 paper submissions this year even though the negative effect of the pandemic still persists. I also would like to extend my appreciation to the IEEE Turkey Section and First University for their generosity in support of ISDFS 2021, and I would like to take this opportunity to thank Scientific Committee Members for their help during the paper review process.

Sincerely Yours,

June 28th, 2021
Prof. Dr. Asaf Varol
General Coordinator of ISDFS

ORGANIZING COMMITTEE

Term Chairs of ISDFS-2021

Assoc. Prof. Dr. Fatih Özkaynak, Fırat University, Elazığ, TR

General Chair of ISDFS

Prof. Dr. Asaf Varol, Maltepe University, TR

Co-Chairs and Program Chairs

Assoc. Prof. Dr. Cihan Varol, Sam Houston State University, USA
Assoc. Prof. Dr. Murat KARABATAK, Fırat University, TR

Local Organizing Team

Assoc. Prof. Dr. Fatih Özkaynak, Fırat University, Elazığ, TR
Assoc. Prof. Dr. Mustafa Ulaş, Fırat University, Elazığ, TR

Conference Registration and Arrangements Committee

Asst. Prof. Dr. Tamer Kavuran, Graphic Design, Firat University, TR
Asst. Prof. Dr. Mehmet KAYA, Conference Arrangements, Syracuse University, USA
Asst. Prof. Dr. Songül Karabatak, Conference Arrangements, Firat University, TR
Res. Asst. Cem Baydoğan, Conference Arrangements, Firat University, TR
Furkan Erdoğan, Web Design and Programming, Firat University, TR

Publications Committee Members

Assoc. Prof. Dr. Cihan Varol, Sam Houston State University, USA

Consortium Members

Prof. Dr. Asaf Varol, Maltepe University, TR
Assoc. Prof. Dr. Fatih ÖZKAYNAK, Fırat University, TR
Prof. Dr. Peter Alan Cooper, Sam Houston State University, US
Prof. Dr. Hamadou Saliah-Hassane, TELUQ University, CA
Prof. Dr. Şeref Sağıroğlu, Gazi University, TR
Prof. Dr. Çetin Arslan, Hacettepe University, TR
Assoc. Prof. Dr. Ayhan İstanbullu, Balıkesir University, TR
Prof. Dr. Maria Manuela Cruz-Cunha, Polytechnic Institute of Cávado and Ave, PT
Assoc Prof. Dr. Mohammad Malli, Arab Open University, LB
Prof. Dr. Milan Tuba, Singidunum University, XS
Prof. Dr. Nizamettin Aydın, Yildiz Technical University, TR
Prof. Dr. Yusuf Öztürk, San Diego State University, USA
Assoc. Prof. Dr. Sedat Akleylek, Ondokuz Mayıs University, TR
Asst. Prof. Dr. İlker Özçelik, Recep Tayyip Erdoğan University, TR
Assoc. Prof. Dr. Murat KARABATAK, Association of Software and Cyber Security of Turkey, TR
Rahmi Aktepe, President of Informatics Association of Turkey, TR

SCIENTIFIC COMMITTEE MEMBERS

First Name	Middle	Last Name	Organization
Abdulsamet		Hasiloglu	Ataturk University, TR
Ahmet		Aydoğan	Sam Houston State, USA
Ahmad		Fadlallah	USAL, LB
Ahmet	Hasan	Koltuksuz	Yasar University, TR
Ali	Aydin	Selçuk	TOBB ETU, TR
Ali		Yazici	Atilim University, TR
Amar		Rasheed	Sam Houston State University, USA
Antal		Margit	Sapientia University, RO
Asaf		Varol	Maltepe University, TR
Atila		Bostan	Atilim University, TR
Ayhan		Erdem	Gazi University, TR
Ayhan		Istanbullu	Balikesir University, TR
Bachar	Ahmed	Elhassan	Lebanese University, LB
Baris		Aksanli	San Diego University, USA
Bassem		Haidar	Public Lebanese University, LB
Bedri		Ozer	Firat University, TR
Bihter		Das	Firat University, TR
Bilal		Alatas	Firat University, TR
Bogdan		Robu	Grenoble Institute of Technology, FR
Bünyamin		Ciylan	Gazi University, TR
Cetin	Kaya	Koc	Istinye University, TR
Chia-Chu		Chiang	University of Arkansas at Little Rock, US
Chris		Bowerman	University of Sunderland, UK
Cihan		Varol	Sam Houston State University, USA
Derya		Avcı	Firat University, TR
Dimitris		Geneiatakis	Aristotle University of Thessaloniki, GR
Ecir	Ugur	Kucuksille	Suleyman Demirel University, TR
Elif		Varol	Firat University, TR
Enis		Karaarslan	Marmara University, TR
Erkan		Tanyildizi	Firat University, TR
Erkay		Savas	Sabanci University, TR
Esref		Adali	ITU, TR
Fahad		Salamh	Purdue University, USA
Fakis		Alexandros	University of the Aegean, GR
Fatih		Ozkaynak	Firat University, TR
Ferruh		Ozbudak	METU, TR
Georgios		Kambourakis	University of the Aegean, GR
Georgios		Karopoulos	University of Athens, GR
Gheorghe		Sebestyen	Technical University of Cluj-Napoca, RO
Hamadou	Saliah	Hassane	Teluq University, CA
Hassan		Noura	Arab Open University, LB
Husrev	Taha	Sencar	TOBB ETU, TR
Ibrahim	Halil	Bulbul	Ahmet Yesevi University, KZ
Ibrahim		Ozcelik	Sakarya University, TR
Ibrahim		Sogukpinar	Gebze Institute of Technology, TR
Ioan		Salomie	Technical University of Cluj-Napoca, RO
Ibrahim		Turkoglu	Firat University, TR
Joao		Vilaça	Polytechnic Institute of Cávado and Ave, PT
Jozsef		Vssarhelyi	University of Miskolc, HU
Kenji		Yoshigoe	University of Arkansas at Little Rock, USA
Lei		Chen	Georgia Southern University, USA
Luis		Ferreira	Polytechnic Institute of Cávado and Ave, PT
Maha	Farouk	Sabir	King Abdulaziz University, SA

Majed		Sinane	Public Lebanese University, LB
Maria Manuela	Cruz	Cunha	Polytechnic Institute of Cávado and Ave, PT
Mehmet		Kaya	Syracuse University, USA
Mohand	Tahar	Kechadi	University College Dublin, IE
Mohammad		Awwad	National Center of Remote Sensing, LB
Mohammad		Malli	Arap Open University, LB
Mohammad		Awwad	Mational Center of Remote Sensing, Lebanon
Mohammad		Sbeiti	Deutsche Telecom, LB
Muhammet		Baykara	Firat University, TR
Muharrem	Tolga	Sakalli	Trakya University, TR
Murat		Karabatak	Firat University, TR
Narasimha K.		Shashidhar	Sam Houston State University, USA
Nazife		Baykal	METU-Cyprus, CY
Nhien-An		Le-Khac	University College Dublin, IE
Nizamettin		Aydın	Yıldız Technical university, TR
Nuno	Mateus	Coelho	Univ. of Trás os Montes e Alto Douro, PT
Nuno		Lopez	Polytechnic Institute of Cávado and Ave, PT
Nuno		Rodrigues	Polytechnic Institute of Cávado and Ave, PT
Osman		Altay	Celal Bayar Universty, TR
Ozal		Yıldırım	Firat University, TR
Ozgur		Karaduman	Firat University, TR
Ozgur		Yurekten	Cumhurbaşkanlığı Dijital Dnüşüm Ofisi, TR
Peter	Alan	Cooper	Sam Houston State University, USA
Raymond		Choo	University of South Australia, AU
Razvan		Deaconescu	Univ. Politehnica of Bucharest, RO
Resul		Das	Firat University, TR
Sandro		Carvalho	Polytechnic Institute of Cávado and Ave, PT
Sedat		Akleylek	Ondokuz Mayis University, TR
Seethal		Paluri	San Diego State University, USA
Selcuk		Kavut	Balikesir University, TR
Sengul		Dogan	Firat University, TR
Seref		Sagiroglu	Gazi University, TR
Sheikh	Ariful	Islam	University of Texas Rio Grande Valley, USA
Songul		Karabatak	Firat University, TR
Sundar		Krishnan	Sam Houston State University, USA
Sunil		Kumar	San Diego State University, USA
Suzanne		McIntosh	New York University, USA
Sylvain		Guilley	Secure-IC S.A.S Rennes, FR
Szabo		Laszlo	Sapientia University, RO
Szanto		Zoltan	Sapientia University, RO
Tolga		Sakalli	Trakya University, TR
Tuncay		Dincer	Ege University, TR
Turker		Tuncer	Firat University, TR
Vajda		Tamas	Sapientia University, RO
Yaman		Akbulut	Firat University, TR
Yunus		Santur	Firat University, TR
Yusuf		Celik	Firat University, TR
Yusuf		Ozturk	San Diego State University, USA
Yusuf		Tulgar	Net Data Soft, TR
Zisis		Tsiatsikas	University of the Aegean, GR

SYMPOSIUM PROGRAM

9TH INTERNATIONAL SYMPOSIUM ON DIGITAL FORENSICS AND SECURITY

28 JUNE 2021, ELAZIĞ – TURKEY

10:00-10:45 **OPENING CEREMONY (ASSOC. PROF. DR. CIHAN VAROL)**

ASSOC. PROF. DR. FATIH OZKAYNAK	TERM CHAIR OF ISDFS-2021, FIRAT UNIVERSITY, TR
PROF. DR. ASAF VAROL	GENERAL CHAIR OF ISDFS, MALTEPE UNIVERSITY, TR
RAHMI AKTEPE	INFORMATICS ASSOCIATION OF TURKEY, TR
PROF. DR. ŞAHIN KARASAR	RECTOR OF MALTEPE UNIVERSITY, TR
PROF. DR. FAHRETTIN GÖKTAŞ	RECTOR OF FIRAT UNIVERSITY, TR

10:45-11:30 **KEYNOTE SPEECH (ASSOC PROF. DR. AHMET KOLTUKSUZ)**

CYBER WARFARE: CHANGING DOCTRINES OF WARFARE FROM SUN TZU TO CYBERSPACE

11:30-12:15 **IN-PERSON AND ONLINE PRESENTATIONS (SESSION CHAIR: PROF. DR. ASAF VAROL)**

PAPER ID 46: A NEW APPROACH TO SOCIAL ENGINEERING WITH NATURAL LANGUAGE PROCESSING: RAKE
AYDOGAN, AHMET FURKAN*; AN, MIN KYUNG; YILMAZ, MEHMET

PAPER ID 63: REVIEW OF NLP- BASED SYSTEMS IN DIGITAL FORENSICS AND CYBERSECURITY
UKWEN, DAVID OKORE*; KARABATAK, MURAT

PAPER ID 10: EDI BASED SECURE DESING PATTERN FOR LOGISTIC AND SUPPLY CHAIN
KARATAS, CEYHUN*; GULTEKIN, MUAZ

PAPER ID 19: GRAPH- BASED MALWARE DETECTION USING OPCODE SEQUENCES
GULMEZ, SIBEL*; SOGUKPINAR, IBRAHIM

12:15-14:00 **SOCIAL EVENT AT FIRAT UNIVERSITY**

14:00-15:00 **ONLINE PRESENTATIONS (SESSION CHAIR: ASSOC. PROF. DR. CIHAN VAROL)**

PAPER ID 16: EXPLOITING VULNERABILITIES OF IP CAMERAS: LEBANON CASE STUDY
BATHICH, PETER; MALLI, MOHAMMAD; HAZIMEH, HUSSEIN*

PAPER ID 38: A NOVEL REVERSIBLE FRAGILE WATERMARKING IN DWT DOMAIN FOR TAMPER LOCALIZATION AND DIGITAL IMAGE AUTHENTICATION
AZIZOĞLU, GÖKHAN*; TOPRAK, AHMET NUSRET

PAPER ID 58: A COMPARATIVE STUDY ON THE DETECTION OF IMAGE FORGERY OF TAMPERED BACKGROUND OR FOREGROUND
ELMACI, MEHMET*; TOPRAK, AHMET NUSRET; ASLANTAS, VEYSEL

15:00-16:30 **PANEL SPEECH (TBD INFORMATICS VISION PANEL)**

MODERATOR ANS SPEAKER:

CENK TEZCAN (B-WISE CO-FOUNDER) **: BUSINESS LIFE OF THE FUTURE**

SPEAKERS :

CEMIL ŞINASI TÜRÜN : NEW FINANCIAL SYSTEMS

DR. ZIYA KARAKAYA : CLOUD COMPUTING

MURAT LOSTAR : CYBER SECURITY

16:30-17:15 **ONLINE PRESENTATIONS (SESSION CHAIR: PROF. DR. ASAF VAROL)**

PAPER ID 27: A COST-EFFECTIVE SECURITY FRAMEWORK TO PROTECT MICRO ENTERPRISES: PALANTIR E-COMMERCE USE CASE
MLAKAR, IZIDOR*; JERAN, PRIMOŽ; ŠAFRAN, VALENTINO; LOGOTHETIS, VANGELIS

PAPER ID 39: THREAT LANDSCAPE EXPANSION DURING COVID-19: REMOTE INCIDENT RESPONSE HANDLING
WILLIAMS, FRANK*; VAROL, CIHAN; RASHEED, AMAR A; SHASHIDHAR, NARASIMHA

PAPER ID 55: AUTOMATED MALWARE DESIGN FOR CYBER PHYSICAL SYSTEMS
TANTAWY, ASHRAF*

17:15-18:00 **KEYNOTE SPEECH (NICOLAS HUGHES)**

A TIME OF RECKONING? CHANGING REGULATORY AND JUDICIAL ATTITUDES AND THE POTENTIAL IMPACT ON DIGITAL FORENSICS

OFFLINE PRESENTATIONS

SPECIAL SESSION: P2834

PAPER ID 28: EVALUATION OF BLOCKCHAIN TECHNIGUES TO ENSURE SECURE ACCESS ON REMOTE FPGA LABORATORIES
WERNER, EMILIO*; BEREJUCK, MARCELO DANIEL D; MATIAS, JHENNIFER CRISTINE; SALIAH-HASSANE, HAMADOU

PAPER ID 59: PREVENTION PRE-VIOLENCE IN E-LABS WITH MACHINE LEARNING: PVE
AYDOGAN, AHMET*; SHASHIDHAR, NARASIMHA

CYBER SECURITY

PAPER ID 11: BLOCKCHAIN-BASED IOT: AN OVERVIEW
VAROL, ASAF; RAZA, MUHAMMAD RAHEEL*; HUSSAIN, WALAYAT

PAPER ID 12: PQ-FLAT: A NEW QUANTUM-RESISTANT AND LIGHTWEIGHT AUTHENTICATION APPROACH FOR M2M DEVICES
KARACAN, ENGIN*; AKLEYLEK, SEDAT; KARAKAYA, AYKUT

PAPER ID 17: ANALYSIS AND MODELING OF CYBER SECURITY PRECAUTIONS
DURMUŞ, OMER*; VAROL, ASAF

PAPER ID 23: CLOCK GATING- ASSISTED MALWARE (CGAM): LEVERGING CLOCK GATING ON ARM CORTEX M* FOR ATTACKING SUBSYSTEMS AVAILABLITY
RASHEED, AMAR A*; VAROL, HACER; BAZA, MOHAMED

PAPER ID 31: MITRE ICS ATTACK SIMULATION AND DETECTION ON ETHERCAT BASED DRINKING WATER SYSTEM
TOKER, FIRDEVS S*; OVAZ AKPINAR, KEVSER; OZCELIK, IBRAHIM

PAPER ID 32: CENTER WATER: A SECURE TESTBED INFRASTRUCTURE PROPOSAL FOR WASTE AND POTABLE WATER MANAGEMENT
OVAZ AKPINAR, KEVSER; OZCELIK, IBRAHIM; ISKEFIYELI, MURAT; BALTA, MUSA*; TOKER, FIRDEVS S

PAPER ID 34: A COST BASED DYNAMIC RESPONSE METHOD FOR INTERNET OF THINGS CYBERATTACKS
CHOUHAN, PUSHPINDER K*; QUIGLEY, BRONAGH; BEARD, ALFIE; CHEN, LIMING

PAPER ID 36: MALWARE DETECTION AND CLASSIFICATION USING FASTTEXT AND BERT
YESIR, SALIH*; SOGUKPINAR, IBRAHIM

PAPER ID 48: A NOVEL RISK MITIGATION & CLOUD- BASED DISASTER RECOVERY FRAMEWORK FOR SMALL TO MEDIUM SIZE BUSINESSES
SOLIS, ROBERTO*; SHASHIDHAR, NARASIMHA; VAROL, CIHAN

PAPER ID 49: ANALYSIS OF NETWORK PROTOCOLS FOR SECURE COMMUNICATION
ISLAM, SHEIKH ARIFUL*; CABALLERO, DAVID; GONZALEZ, FRANCISCO

PAPER ID 53: A DATA MINING BASED SYSTEM FOR AUTOMATING CREATION OF CYBER THREAT INTELLIGENCE
ARIKAN, SULEYMAN MUHAMMED*; ACAR, SAMI

CRYPTOGRAPHY

PAPER ID 42: A SUBSTITUTION-BOX STRUCTURE BASED ON CROWD SUPPLY INFINITE NOISE TRNG
IBRAHIM, HABIB*; OZKAYNAK, FATIH

DATA PRIVACY

PAPER ID 07: CAPEN: CRYPTOGRAPHIC ACCUMULATOR BASED PRIVACY PRESERVING EXPOSURE NOTIFICATION
OZCELIK, ILKER*

DIGITAL FORENSICS

PAPER ID 05: WATERMARKING GRAPH NEURAL NETWORKS BY RANDOM GRAPHS
WU, HANZHOU*; ZHAO, XIANGYU; ZHANG, XINPENG

PAPER ID 06: SELECTING THE BEST FORENSIC REPORT BY USING A GROUP DECISION MAKING METHOD: A CASE STUDY ON THREE FORENSIC REPORTS
AKKUZU KAYA, GULSUM*; BADWAN, ABDUL

PAPER ID 33: METHOD FOR PROTECTION OF HETEROGENEOUS DATA BASED ON PSEUDO-HOLOGRAPHIC WATERMARKS
VYBORNOVA, YULIYA*

PAPER ID 35: DEVELOPMENT AND MAINTENANCE OF MOBILE FORENSIC INVESTIGATION SOFTWARE MODULES
ARIKAN, SULEYMAN MUHAMMED*; YUREKTEN, OZGUR

COMPUTER SCIENCE

PAPER ID 02: A SYMPTOM-BASED MACHINE LEARNING MODEL FOR MALARIA DIAGNOSIS IN NIGERIA
BILYAMINU, MUHAMMAD*; VAROL, ASAF

PAPER ID 18: SENTIMENT ANALYSIS USING DEEP LEARNING IN CLOUD
VAROL, ASAF; HUSSAIN, WALAYAT; RAZA, MUHAMMAD RAHEEL*; TANYILDIZI, ERKAN

PAPER ID 20: PREDICTION OF ARRHYTHMIA WITH MACHINE LEARNING ALGORITHMS
GURSOY, GUNES*; VAROL, ASAF

PAPER ID 22: MODELING AND FORECASTING OF TOURISM TIME SERIES DATA USING ANN-FOURIER SERIES MODEL AND MONTE CARLO SIMULATION
DANBATTA, SALIM JIBRIN*; VAROL, ASAF

PAPER ID 25: TTSD: A NOVEL DATASET FOR TURKISH TEXT SUMMARIZATION
ULKER, MEHTAP*; OZER, A. BEDRI

PAPER ID 26: FUZZY RULE BASED CLASSIFICATION SYSTEM FROM VEHICLE-TO-GRID DATA
AKKUZU KAYA, GULSUM*; BADWAN, ABDUL

PAPER ID 44: A BRIEF SURVEY ON RANSOMWARE WITH THE PERSPECTIVE OF INTERNET SECURITY THREAT REPORTS
FARHAT, DANYAL*; AWAN, MALIK SHAHZAD

PAPER ID 50: DETECTION OF WEB ATTACKS VIA PART CLASSIFIER
AHMED, OMAR ISKNDAR*; VAROL, CIHAN

PAPER ID 56: ENTERPRISE INFORMATION SYSTEMS ENHANCEMENT: HYPERLEDGER FABRIC BASED APPLICATION
BOURAS, ABDELAZIZ; GASMI, HOUSSEM; BELHI, ABDELHAK*; HAMMI, ASSAM; AOUNI, BELAID

PAPER ID 60: A STUDY OF SEMICONDUCTOR DEFECTS WITHIN AUTOMOTIVE MANUFACTURING USING PREDICTIVE ANALYTICS
VAROL, SERKAN; O'DOUGHERTY, PATRICK*; FERREL, KEITH

PAPER ID 61: INVESTIGATION OF SELF- DIRECTED LEARNING SKILLS OF DISTANCE EDUCATION STUDENTS
ALANOGLU, MUSLIM*; KARABATAK, SONGUL; KARABATAK, MURAT

PAPER ID 62: PROBLEMS ENCOUNTERED IN DISTANCE TEACHING PRACTICES COURSE AND SOLUTION SUGGESTIONS
ALANOGLU, MUSLIM*; KARABATAK, SONGUL; KARABATAK, MURAT

PAPER ID 64: EARTHQUAKE PREDICTION BY USING TIME SERIES ANALYSIS
LOK, SULTAN*; KARABATAK, MURAT

PAPER ID 65: A NEW SUSTAINABLE HYBRID SOFTWARE DEVELOPMENT METHODOLOGY: FIRAT-UG
ULAS, MUSTAFA*; GULER, HAKAN

PAPER ID 66: SOFTWARE ENGINEERING FOR DATA MINING (ML- ENABLE) SOFTWARE APPLICATIONS
SAEED, SABEER*; ABUBAKAR, MOHAMMED MANSUR; KARABATAK, MURAT

ABSTRACTS

Paper ID: 02
A Symptom-Based Machine Learning Model for Malaria Diagnosis in Nigeria

Muhammad Bilyaminu*, Asaf Varol

* Usmanu Danfodiyo University, NIGERIA
*Email: bilyaminu49@gmail.com

***Abstract*—** Malaria, with around 200 million cases worldwide, tends to kill more people than war and crises. With efforts to reduce mortality rates being futile, an inadequate malaria diagnosis is one of the barriers to a successful reduction in mortality. Machine learning methods were used to classify the stages of malaria in patients to improve diagnosis. To predict the stages of malaria, this research used knowledge of an algorithm of machine learning for a predictive model. A 77% accurate decision algorithm was developed using the symptoms of patients to identify their malaria stages. This research also discovered that malaria does not kill only children (between 0–5 years), in contrast to what has been pointed out in many research studies. This study shows that older women are more likely to experience severe stages of malaria. Therefore, adequate care should be considered for these women once they show some of the significant symptoms as described in the model. This approach applies to everyone with the symptoms set out in the model. This system will provide a preliminary test before conducting a confirmatory diagnosis in the laboratories.

Paper ID: 05
Watermarking Graph Neural Networks by Random Graphs

Xiangyu Zhao*, Hanzhou Wu, Xinpeng Zhang

*Shanghai University, CHINA
*Email: 3286340865@qq.com

***Abstract*—** Many learning tasks require us to deal with graph data which contains rich relational information among elements, leading increasing graph neural network (GNN) models to be deployed in industrial products for improving service quality. However, they also raise challenges to model authentication. It is necessary to protect the ownership of the GNN models, which motivates us to watermark GNN models. In this work, an Erdos-Renyi (ER) random graph with random node feature vectors and labels is randomly generated as a trigger to train the GNN to be protected together with the normal samples. During model training, the secret watermark is embedded into the label predictions of graph nodes. During model verification, by activating a marked GNN with the trigger ER graph, the watermark can be reconstructed from the output to verify the ownership. Since the ER graph was randomly generated, by feeding it to a non-marked GNN, the label predictions of graph nodes are random, resulting in a low false alarm rate (of proposed work). Experimental results have also shown that, the performance of a marked GNN on its original task will not be impaired. And, it is robust against model compression and fine-tuning, which has shown superiority and applicability.

Paper ID: 06
Selecting the Best Forensic Report by Using a Group Decision Making Method: A case study on three forensic reports

Gülsüm Akkuzu Kaya*, Abdul Badwan

*Recep Tayyip Erdoğan University, TURKEY
*Email: gulsum.akkuzukaya@erdogan.edu.tr

***Abstract*—** Group decision making (GDM) techniques have been very popular to take the best and the most convenient decision from an alternative set. GDM techniques have been applied in various area of information sharing as well as forensic information sharing. In a forensic investigation process, different forensic reports are produced by different investigators. Produced forensic reports are taken to the court as a file of evidence however deciding which report should be taken to the court is a challenging. Because decision is single handed, officer makes decision. There are two main approaches s/he might follow in selection; the first one is to combine the forensic reports into one report if investigators are located in the same environment, the other one is to choose the most comprehensive report (individually decided). Both approaches may cause continuance by undue process because of insufficient evidence because reports which are not taken to the court might include the needed evidence. In order to solve such problems in forensic area, this work provides a consensus-reached GDM approach in which extended induced ordered weighted average technique is used. Three forensic master students' forensic reports are used for application of the work. The result of the application phase showed that consensus-reached GDM makes the taken decision better and more accurate.

Paper ID: 07
CAPEN: Cryptographic Accumulator based Privacy Preserving Exposure Notification

İlker Özçelik*

* Recep Tayyip Erdoğan University, TURKEY
*Email: ozcelikilker@ieee.org

***Abstract*—** Contact tracing has a significant contribution in preventing the rapid spread of infectious diseases. During the COVID-19 pandemic, local authorities, researchers and the tech industry focused on developing digital contact tracing applications to automate tracing efforts and improve its efficiency. While digital contact tracing was proven to be an efficient method to mitigate transmission, the security and privacy of the user data remains a major concern. In this paper we focused on digital tracing application data privacy issues and proposed Cryptographic Accumulator based Privacy Preserving Exposure Notification module (CAPEN). In the CAPEN module we used an asymmetric cryptographic accumulator and greatest common divisor (gcd) function to provide privacy for the user data while providing accurate verification. Additionally, the CAPEN module has a significantly lower communication complexity while sharing larger datasets. The CAPEN module is architecture independent and can be easily incorporated with any digital contact tracing system in order to prevent enumeration and social graph attacks without compromising contact verification accuracy.

Paper ID: 10
EDI Based Secure Desing Pattern For Logistic and Supply Chain

Ceyhun Karataş*, Muaz Gültekin

* Barsan Global Logistic, TURKEY
*Email: ceyhun.karatas@barsan.com

Abstract— In ERP's (Enterprise Resource Planning)) integration processes, different solutions are used for data exchange. ERPs can be customized according to the solution used in the integration process. Due to use of different data types, systems can become complex. This complexity leads to problems with regards to data security. There still may be inadequate and missed conditions despite security measures taken for each data exchange method. Currently, EDI (Electronic Data Interchange) is one of the most widely used solutions for Data Exchange. In this study, we have created a design pattern that supports all kinds of data exchange and offers a holistic security solution. In this model, EDI is designed as intermediate level. A flexible and secure model is presented to ERP systems with this solution.

Paper ID: 11
Blockchain- Based IoT: An Overview

Asaf Varol, **Muhammed Raheel Raza***, Walayat Hussein

*COMSATS University, PAKISTAN
*Email: 191137125@firat.edu.tr

Abstract— The Internet of Things (IoT) has revolutionized the human world by transforming ordinary everyday objects into smart devices. These autonomous devices have reshaped our lives. The emerging technology is expanding day-by-day with the increasing need for smart devices as so the issues are also increasing w.r.t security, data reliability, maintenance and authentication. On the other hand, another innovative technology- Blockchain- has transformed our financial world by introducing sophisticated security. An integrated Blockchain-IoT system can resolve the problems they face individually and serve the technological world better. The paper provides a comprehensive study of both technologies by highlighting their features and challenges. The article further critically analyses existing approaches that discussed various issue about IoT and Blockchain.

Paper ID: 12
PQ- Flat: A new Quantum- Resistant And Lightweight Authentication Approach for M2M Devices

Engin Karacan*, Sedat Akleylek, Aykut Karakaya

* 19 Mayıs University, TURKEY
*Email: enginkaracan@gmail.com

Abstract— It is believed that traditional asymmetric cryptosystems are compromised and symmetric cryptography can be used in the post-quantum world. In this paper, a new model based on post-quantum a set of FLAT (PQ-FLAT) protocol is proposed to ensure security in the machine to machine communication with post-quantum cryptography and it is inspired by the federated lightweight authentication of things (FLAT) protocol, which works effectively for resourceconstrained devices in machine to machine (M2M) communication systems. The proposed model includes resourceconstrained devices, certificate provider (CP), and service provider (SP). Communication of the certificate provider between resource-constrained devices is encrypted with AES. Instead of the asymmetric cryptography system between the certificate provider and the service provider, a lattice-based encryption mechanism, secure in the post-quantum world, is used. Thus, the FLAT protocol for resource-constrained devices is made resistant to post-quantum changes.

Paper ID: 16
Exploiting Vulnerabilities of IP Cameras: Lebanon Case Study

Hussein Hazimeh*, Peter Bathich, Mohammed Malli,

*Arap Open University, LEBANON
*Email: hhazimeh@aou.edu.lb

***Abstract*—** As applications and devices in the Internet of Things (IoT) increasingly grow, the protection and privacy of IoT devices has been a significant issue. In addition, in many cases there are no security protocols for the defense of these devices that can be a best place for the attacker to take advance of these vulnerabilities which can cause many damage in the level of availability, integrity and privacy of the users in many types of IoT devices. For control and connectivity to their computers, users of IoT devices use the internet. The usage of IoT technology has massively grown over time. Some statistic show that in the end of 2021 the number of these devices can reached 50 billions, we are constantly and unwittingly collecting our sensitive data via IoT devices. In this paper, we present a case study about the IP cameras used in Lebanon and the most vulnerabilities that affect such devices.

Paper ID: 17
Analysis and Modeling of Cyber Security Precautions

Ömer Dumuş*, Asaf Varol

*Samsun University, TURKEY
*Email: omer.durmus@samsun.edu.tr

Abstract— Taking security measures against cyber-attacks has become a necessity for the whole world. Determining the most appropriate measures and their effective implementation form the basis of cyber security for all key institutions. This study, aims to demonstrate the appropriate analysis of cyber-attacks and analysis output models that facilitate fast and effective interventions. An understandable scenario was created by applying statistical calculation methods to the analysis output models and thanks to this work a new model was provided for an effective and significant cyber security intervention. Studies have been carried out on data sets belonging to 2020 and covering many cyber-attacks, having a sampling space for network, software and different hardware attacks, and the structured output of the data analysis has been modeled with SPSS.

Paper ID: 18
Sentiment Analysis using Deep Learning in Cloud

Asaf Varol, **Mohammad Raheel Raza***, Walayat Hussain, Erkan Tanyıldızı

*COMSATS University, PAKISTAN
*Email: 191137125@firat.edu.tr

Abstract— Sentiments are the emotions or opinions of an individual encapsulated within texts or images. These emotions play a vital role in the decision-making process for a business. A cloud service provider and consumer are bound together in a Service Level Agreement (SLA) in a cloud environment. SLA defines all the rules and regulations for both parties to maintain a good relationship. For a long-lasting and sustainable relationship, it is vital to mine consumers' sentiment to get insight into the business. Sentiment Analysis or Opinion Mining refers to the process of extracting or predicting different point of views from a text or image to conclude. Various techniques, including Machine Learning and Deep Learning, strives to achieve results with high accuracy. However, most of the existing studies could not unveil hidden parameters in text analysis for optimal decision-making. This work discusses the application of sentiment analysis in the cloud-computing paradigm. The paper provides a comparative study of various textual sentiment analysis using different deep learning approaches and their importance in cloud computing. The paper further compares existing approaches to identify and highlight gaps in them.

Paper ID: 19
Graph- Based Malware Detection Using Opcode Sequences

Sibel Gülmez*, İbrahim Soğukpınar

*Gebze Technical University, TURKEY
*Email: sgulmez2018@gtu.edu.tr

Abstract— The impact of malware grows for IT (information technology) systems day by day. The number, the complexity, and the cost of them increase rapidly. While researchers are developing new and better detection algorithms, attackers are also evolving malware to fail the current detection techniques. Therefore malware detection becomes one of the most challenging tasks in cyber security. To increase the performance of the detection techniques, researchers benefit from different approaches. But some of them might cost a lot both in time and hardware resources. This situation puts forward fast and cheap detection methods. In this context, static analysis provides these utilities but it is important to keep detection accuracy high while reducing resource consumption. Opcodes (operational codes) are commonly used in static analysis but sometimes feature extraction from opcodes might be difficult since an opcode sequence might have a great length. Furthermore, most of the malware developers use obfuscation and encryption techniques to avoid detection methods based on static analysis. This kind of malware is called packed malware and according to common belief, packed malware should be either unpacked or analyzed dynamically in order to detect them. In this study, a graph-based malware detection method has been proposed to overcome theseproblems. The proposed method relies on obtaining the opcode graph of every executable file in the dataset and using them for future extraction. In this way, the proposed method reaches up to 98% detection accuracy. In addition to the accuracy rate, the proposed method makes it possible to detect packed malware without the need for unpacking or dynamic analysis.

Paper ID: 20
Prediction of Arrhythmia with Machine Learning Algorithms

Güneş Gürsoy*, Asaf Varol

*Maltepe University, TURKEY
*Email: gunesgursoy@hotmail.com

Abstract— The present study uses the age, sex, diabetes mellitus, and arrhythmia data of patients from the datasets presented in an existing study to predict arrhythmia with machine learning algorithms, K-Nearest Neighbors (KNN), and Naive Bayes methods. The outputs are schematically presented, and the conclusions related to the Bayes theorem and KNN algorithms are compared. In the case of increasing the value of neighboring k in the KNN method, it is seen that the accuracy rate approaches the result obtained from the Naive Bayes method.

Paper ID: 22
Modeling and Forecasting of Tourism Time Series Data using ANN- Fourier Series Model and Monte Carlo Simulation

Salim Jibrin Danbatta*, Asaf Varol

*Kano State Institute for Information Technology, NIGERIA
*Email: salimdambatta@gmail.com

Abstract— Tourism is counted as one of the most sensitive sectors to crises such as the COVID-19 pandemic. By the first quarter of 2020, it brought the foreign visitors' travels to a sudden and unexpected halt. This has negatively affected the tourism sector. Due to the perishable nature of the tourism industry products, many researchers are calling for urgent development and implementation of a rescue plan that will help in predicting the future number of foreign visitors. In this paper, we proposed an approach to modeling and forecasting a tourism time-series data that have both trend and seasonality. This approach is a combination of the Fourier series and artificial neural network methods to capture the seasonality and trend components in data. We applied this method to the monthly foreign visitors to Turkey dataset. We studied the data for the periods before, and during the COVID-19 pandemic. To account for uncertainties in the model prediction during the COVID-19 pandemic, we employed the Monte Carlo simulation method. We run 100 Monte Carlo simulations within $\pm 2\sigma$ from the model curve. The mean of these 100 Monte Carlo simulation paths is computed and used for presenting the Monte Carlo forecast result values of the data. To test the feasibility of this approach, we compared the model predictions with some other existing models in the literature. In each case, the model has demonstrated a decent prediction and outperformed the benchmarked models. The proposed model produces a statistically good fit and acceptable result that can be used to forecast other tourism-related attributes.

Paper ID: 23
Clock Gating- Assisted Malware(CGAM): Leverging Clock Gating on ARM Cortex M* For Attacking Subsystems Availability

Amar A. Rasheed*, Hacer Varol, Mohamad Baza

* Sam Houston State University, USA
*Email: amarrasheed@gmail.com

Abstract— Due to the ever-increasing demand for developing Internet of Things (IoT) technologies that support low power consumption and high-performance mobile computing, several power optimization techniques have been implemented and deployed at the processors level, especially the ARM Cortex-M family chipsets. Such techniques include clock gating, power gating, dynamic voltage, and frequency scaling. Although such mechanisms help in minimizing dynamic power consumption by shutting off current to blocks or chip-operational units that are not in use, power gating and clock-gating techniques can be exploited by an attacker to disable blocks within the chipset targeting the subsystem availabilities. Attacks include disabling serial communication blocks, wireless/ethernet communication modules, Random Number Generator (RNG) block, interrupt module, etc. This paper proposed the development of a live clockgating assisted malware attack for IoT systems based on the ARM Cortex-M processor. Four variants of the proposed malware were codded and deployed on a real IoT testbed integrated with a multisensor data fusion algorithm. Behavioral patterns based on power spectral density estimations and current measurements were recorded for each strain of the proposed malware. In thisresearch, collected behavioral patterns were utilized to identify an infected device and its injected malware strain.

Paper ID: 25
TTSD: A Novel Dataset For Turkish Text Summarization

Mehtap Ülker*, A. Bedri Özer

* Fırat University, TURKEY
*Email: m.ulker@firat.edu.tr

Abstract— Nowadays, with the increase in the amount of data on the internet, it becomes extremely important to collect salient information from these data efficiently. Gathering and comprehending essential information from such tremendous data as soon as possible is a complex and challenging process for people. Many methods have been proposed to cope with this process. Automatic text summarization systems are one of these methods in term of the fact that it facilitates obtaining the required documents by eliminating the lack of resources and time. Most of these methods are evaluated in datasets which exist in the literature. For Turkish text summarization, it is not enough datasets. In this study, we presented a novel dataset (TTSD-Turkish Text Summarization Dataset) in order to be preferred both in extractive and in abstractive methods. It is evaluated with TextRank, Lexrank, LSA-based, Luhn and Random methods by using sumy package, is compared performances using ROUGE. It is obtained that the proposed dataset has successful results in each method.

Paper ID: 26
Fuzzy Rule Based Classification System from Vehicle-to-Grid Data

Gülsüm Akkuzu Kaya*; Abdul Badwan

*Recep Tayyip Erdoğan University, TURKEY
*Email: gulsum.akkuzukaya@erdogan.edu.tr

Abstract— Vehicle-to-Grid (V2G) system is becoming a very popular concept since it has various benefits such as reducing energy consumption, being environmental friendly, bi-directional charging, and load balancing. Although, it gets highly remarkable and has many advantages, V2G system's security is extremely challenging. Any security flaw in V2G system can cause serious issues on the system. Security issues might open doors to severe damages on the system. One of the most danger damage on such systems is disclosed confidential information. This work therefore analyses what are confidential information features in a V2G system, it then analyses whether a V2G system is vulnerable to attacks or not if the system's confidential information is revealed. To do that, this study used fuzzy-classification technique in which a fuzzy system is developed. It also applied SVM and NB classification techniques in order to compare applied classification techniques in terms of their performances. Comparison results showed that fuzzy-classification technique performed better than other two techniques.

Paper ID: 27
A Cost-Effective Security Framework to protect micro enterprises: PALANTIR e-commerce use case

İzidor Mlakar*, Primož Jeran, Valentino Šafran, Vangelis Logothetis

* University of Maribor, SLOVENIA
*Email: izidor.mlakar@um.si

Abstract— This paper outlines the PALANTIR framework to assist small (SME) and micro enterprises (ME) with a holistic approach towards securing their infrastructure. The platform will deliver a Risk Assessment platform enabling informed decisions related to cybersecurity investment. As highlighted through the described use-case, the PALANTIR will protect the infrastructure and resources with Threat Intelligence as advanced AI Models exploiting threat sharing, are delivered in SecaaS mode. The Remediation Engine will deliver a tailored solution enabling each owner of the SME/ME to design a policy best fittedto their values and requirements. Overall, the Cloud SecaaS deployment of PALANTIR will provide SMEs/MEs with a costefficient mechanism to achieve and maintain adequate levels of protection.

Paper ID: 28
Evaluation of Blockchain Techniques to Ensure Secure Access on Remote FPGA Laboratories

Emilio Werner*, Jhennifer Cristine Matias, Marcelo Daniel Berejuck, Hamadou Saliah- Hassane

*Federal University of Santa Catarina, BRAZIL
*Email: Emilio.werner@ieee.org

Abstract— Laboratories are part of the learning process of students from the most diverse areas of knowledge. However many problems related to physical accessibility and resources become a challenge for teachers and educational institutions. These disadvantages make remote labs, especially computingoriented labs such as FPGA labs, become very popular in the current scenario. It happens because these labs provide a faster way to guarantee quality results equal to the physical model, reducing costs and offering access to students who did not have access to the labs. However, the security system must be implemented and improved continuously, following the advance of technology. This work aims to develop a security and access control system for remote labs using blockchain techniques to standardize and keep the security process up-to-date with new security techniques. The primary authentication processes, authorization and second verification are discussed and adapted for the remote experimentation scenario. This research is part of an ongoing project to create a security system for remote FPGA labs. At the end of the project, we hope to deliver a functional FPGA platform with standardized security processes following blockchain techniques. The project has researchers from the Laboratory at Distance (L@d) of the TÉLUQ University in Montreal, Canada and the Remote Experimentation Laboratory (RExLab) of the Federal University of Santa Catarina (UFSC) Brazil collaborating.

Paper ID: 31
MITRE ICS Attack Simulation and Detection on EtherCAT Based Drinking Water System

Firdevs Sevde Toker*, Kevser Ovaz Akpınar, İbrahim Özçelik

*Sakarya University, TURKEY
*Email: firdevstoker@sakarya.edu.tr

Abstract— Industrial control systems (ICSs) are complex systems due to the technology and protocol diversity they contain. Operational Technology (OT), an ICS operating structure, has different performance and security requirements than the standard IT infrastructure. ICS systems consist of field devices where operational processes take place and control systems that provide management of these devices. Attackers are involved in the whole process after gaining access from the control layer. As a result, critical infrastructure systems are threatened by cyber-attacks. Therefore, continuous monitoring and security audits are also necessary processes for critical infrastructures. In this study, studies on the cyberattack and detection system were carried out on the critical infrastructures of the water management process. On the EtherCAT-based water management process, six different attack vectors for field devices were developed by the techniques in the MITRE ICS ATT&CK matrix, and these attacks were separated by data obtained from network traffic and determined by the SVM algorithm. Attack scenarios were created by selecting seven different MITRE ICS ATT&CK matrix techniques for attacks on the SCADA system in the control center via the engineering computer on the same process. Wazuh HIDS was used for the intrusion detection system for the SCADA system. Visualization of both attacks was done on ELK.

Paper ID: 32
Center Water: A Secure Testbed Infrastructure Proposal For Waste and Potable Water Management

İbrahim Özçelik, Murat İskefiyeli, **Musa Balta*,** Kevser Ovaz Akpınar, Firdevs Sevde Toker

*Sakarya University, TURKEY
*Email: mbalta@sakarya.edu.tr

Abstract— Due to Industrial Control System (ICS)'s critical location, any compromise in their security can have serious consequences. The resilience of ICSs has become a crucial concern to administrators and governments following widely publicized cybersecurity incidents. The inability to apply traditional Information Technology (IT) security practice to ICSs further compounds challenges in adequately securing critical systems. Therefore, there is a need to have a SCADA testbed for checking vulnerabilities and validating security solutions. This paper presents a secure testbed infrastructure for waste and potable water management. The testbed is established under the critical infrastructures national testbed center (CENTER) for training, security research, and attack/defense analysis/tests. Waste and potable water processes support multiple ICS protocols such as DNP3, S7, EtherCAT, Modbus. Each station in the processes is autonomously controlled by local RTUs/PLCs and secured by firewalls with a segregated network. Alternative applications can be made by selecting scenarios with the developed SCADA applications. Also, it provides a robust experimental environment due to its features such as monitoring of both systems, logging, cyber-attack detection.

Paper ID: 33
Method for Protection of Heterogeneous Data based on Pseudo-Holographic Watermarks

Yuliya Vybornova*

*Samara National Research University, RUSSIA
*Email: vybornovamail@gmail.com

Abstract— This paper proposes a comprehensive solution for protection of heterogeneous two-dimensional and threedimensional graphic data from unauthorized distribution and illegitimate changes using pseudo-holographic watermarks. A pseudo-holographic image is a signal, which encodes a binary sequence in the form of sinusoidal functions. The previous research of pseudo-holograms has shown that they are compatible with various popular embedding strategies and besides allow to significantly increase robustness of original watermarking scheme. In this paper, the robustness and information capacity of pseudo-holograms are significantly increased by minimizing the aliasing effect, which occur when the watermark is cropped. For this, a new algorithm for amplitude peak detection is proposed. The approach is based on signal oversampling before DFT calculation and isolating each ring during spectrum analysis. The experimental study has shown the efficiency of a new detection algorithm. The proposed solution allows to select the parameters in such a way as to maintain the resistance to cropping at a givenlevel.

Paper ID: 34
A Cost Based Dynamic Response Method for Internet of Things Cyberattacks

Pushpinder Kaur Chouhan*, Brunagh Quigley, Alfie Beard, Liming Chen

*Ulster University, UK
*Email: pichouhan@ulster.ac.uk

Abstract— Internet of Things (IoT) applications have attracted growing attention due to the widespread availability of low-cost, high power computing devices supported by the latest mobile, wireless and edge technologies. Consequently, this has given rise to new opportunities for cyberattacks, both in sophistication and scale. Prior research has predominantly focused on detecting cyberattacks in real time, while attack mitigation is left to security experts, which is usually both time consuming and requires complex decision-making skills like prioritization and the trade-off of impacts and costs. Recently, research has been directed towards deploying automated responses, with these systems mostly employing static rule-based response selection methodologies. In this paper, we present a novel cost-based response selection method for detected attacks, which is both adaptive and dynamic, addressing the importance of attack and host characteristics within response selection. The methodology is tested and evaluated in a use case, in a real-world IoT scenario, demonstrating its effectiveness.

Paper ID: 35
Development and Maintenance of Mobile Forensic Investigation Software Modules

Süleyman Muhammed Arıkan*, Özgür Yürekten

*TUBİTAK BİLGEM, TURKEY
*Email: suleyman.arikan@tubitak.gov.tr

Abstract— Nowadays, mobile devices are indispensable for social and business activities. Therefore, mobile device forensic technologies are critical for forensics practitioners. While using these technologies, they can investigate and analyze mobile phone application artifacts that contain data useful metadata, such as geographical location and timestamp. However, developing a complete forensic investigation software for mobile devices is challenging. While developing or maintaining forensic investigation software, project team must consider new trends such as emerging IT technologies, increases of popular mobile applications, new features added to existing mobile applications, and security constraints constantly. In this study, we have defined and applied a process based on agile methodology to develop forensic investigation modules. Moreover, we have presented the implementation details of modules for 9 popular Android social media and instant messaging applications, including wireless communication and system information. Finally, we have summarized the difficulties encountered in this study.

Paper ID: 36
Malware Detection and Classification Using fastText and BERT

Salih Yesir*, İbrahim Soğukpınar

*Gebze Technical University, TURKEY
*Email: syesir2018@gtu.edu.tr

Abstract— Among the types of cyber-attacks, malware that causes high financial losses for institutions and individuals is the biggest threat to computer systems. Kinds of malware increase day-by-day and new types are released, which can easily infect our computers through injection vectors such as e-mail, websites, web applications that we use constantly. It is very important to automatically detect them and protect our computer systems against malware threats. Analysis methods are available to protect our computer systems against malware threats. Dynamic analysis is highly effective in obtaining behavioral information of the software on the computer system and can obtain the API call sequence information of the malware. However, the API call sequence can be too long and difficult to understand. This paper proposes subjects the API call sequence to the purification and optimization process. This behavior information is used for the automatic classification task and then used for classification and word representation tasks using the fastText and BERT algorithms. It was used on three different open data sets to see the success of the method. The fastText model performed better than the BERT model in classification and detection tasks.

Paper ID: 38
A novel reversible fragile watermarking in DWT domain for tamper localization and digital image authentication

Gökhan Azizoğlu*, Ahmet Nusret Toprak

*Sivas Cumhuriyet University, TURKEY
*Email: gazizoglu@cumhuriyet.edu.tr

Abstract— In recent years, altering and tampering with digital images have become easier with the swift development of internet and computer technologies. Therefore, the use of image authentication in legal cases, digital forensic, and medical imaging has become of paramount importance. In this paper, as a solution to this problem, we propose an MD5 Hash-based blind reversible fragile watermarking method. We divide the input image into nonoverlapped 4×4 blocks. Then, the watermark information generated from blocks using the MD5 hash function is embedded in the one-level DWT high and middle frequency sub-bands. Our experimental results demonstrate that the proposed method can provide reversibility for applications such as medical, forensic medicine, and military fields where the original image is essential. It can also provide the ability to resist various malicious attacks such as exchange of content, crop, text addition, copy-paste,rotation, content removal, and noise addition.

Paper ID: 39
Threat Landscape Expansion During Covid-19: Remote Incident Response Handling

Frank Williams*, Cihan Varol, Amar Rasheed, Narasimha Shashihar

*Sam Houston State University, USA
*Email: fhw002@shsu.edu

Abstract— This paper provides an automated remote incident handling solution for an Information Security organization that rushed to become work-from-home type businesses because of Covid-19. This paper demonstrates a suitable solution to solve two separate problems. The first problem is to develop a method to enhance both incident response and threat hunting remotely. This is accomplished by developing a triggering mechanism based on the Microsoft Windows Defender antivirus system. The trigger subsequently executes a snapshot of the workstations condition for use by the cybersecurity professionals to determine if this is a false positive or a true positive event. The second problem attempted to solve the issue is to create a local logging mechanism to assist with basic forensics analysis of the remote worker's activity. In a typical enterprise environment, this solution can be utilized efficiently by either a remote desktop protocol or by simply physically picking up the device for further analysis.

Paper ID: 42
A Substitution-Box Structure Based on Crowd Supply Infinite Noise TRNG

İbrahim Habib*, Fatih Özkaynak

*University of Education, GHANA
*Email: habiib30@gmail.com

Abstract— Practical applications in cryptology science have a very wide spectrum. One of the important primitives based on many of these applications is the substitution-box structures. Since substitution-box structures are the main component targeted by many attacks, developing new substitution-box structures resistant to new attack is a hot research topic. Random selectionbased designs have become increasingly popular recently, as they are more resistant to side channel attacks than mathematically based designs. In this study, a random selection-based substitution-box structure is proposed. The proposed substitutionbox is designed based on a true random number generator hardware. Analysis results showed that the proposed substitutionbox has better performance criteria than many designs in the literature. These successful results indicate that the outputs of study can be used successfully in many practical applications that will be designed in the future.

Paper ID: 44
A Brief Survey on Ransomware with the Perspective of Internet Security Threat Reports

Danyal Farhat*, Malik Shahzad Awan

* University of Central Punjab, PAKISTAN
*Email: danyal.farhat@ucp.edu.pk

Abstract— The cyber security has become a mandatory aspect in every industry. The cyber security companies publish threat reports on regular basis. However, their reports are based on internal data and cannot provide complete network attack trends. In this study, we present a survey on malware and ransomware attack trends by using the data obtained from multiple threat reports. We collect, process, and analyze the data to present it in the form of information. The presented information is useful for corporate executives and cyber insurance companies to examine the impact of malware and ransomware attacks in the recent years. As future prospect, we would like to use the presented information to formulate a cyber risk model of ransomware attack. We would like to develop a model to estimate the potential losses of an organization due to a successful ransomware attack.

Paper ID: 46
A New Approach to Social Engineering with Natural Language Processing: RAKE

Ahmet Furkan Aydoğan*, Min Kyung An, Mehmet Yılmaz

*Sam Houston State University, USA
*Email: axa184@shsu.edu

Abstract— Nowadays, with the advancement of technology, the way of thinking of communities has become easily manipulated. Scientific results put forward during the Arab Spring period, which is one of the biggest examples, show that social media is easily used to guide people in different ways. This paper introduces our project, Rake, which has emerged as a method against the aforementioned manipulations. The Rake used Natural Language Processing and Machine Learning algorithms, to generate its own dataset and it consist of three major procedures: Emotion, Reaction, and Word Mapping, Rake is a high performance application that can adapt to areas such as community analysis, business area analysis and advertising. As shown in the experiments, it has achieved a machine learning performance of 94%. In addition, the stages that convey how to adopt the Rake application in large-scale projects were included in the study.

Paper ID: 48
A Novel Risk Mitigation & Cloud-Based Disaster Recovery Framework for Small to Medium Size Businesses

Cihan Varol, **Roberto Solis***, Narasimha Shashidhar

*Sam Houston State University, USA
*Email: rds050@shsu.edu

Abstract— Current guidelines and frameworks for disaster recovery and business continuity focus on helping corporations and large enterprises. With a rising number of vendors offering cloud computing solutions, most small to medium-size businesses do not count on the minimum number of users to qualify for any tier package. Moreover, the cost of purchasing a solution that does not scale to fit the needs of a small business is a consistent issue. Our solution presents a novel framework granting medium to small-size businesses the opportunity to mitigate risk and resume activities after a disaster has taken place. Furthermore, we present several recovery alternatives using a cloud-based storage solution. The results show that an optimal recovery time objective can be achieved by allowing users to retrieve backups from any platform or device with web-browsing capabilities. Also, a high level of integrity on each client can be reached, which lowers the chances of losing data or exposing financial records to an attacker.

Paper ID: 49
Analysis of Network Protocols for Secure Communication

Sheikh Ariful Islam*, David Caballero, Francisco Gonzalez

*University of Texax Rio Grande Valley, USA
*Email: sheikhariful.islam@utrgv.edu

Abstract— In the age of constantly evolving technology, network communication has become more critical than ever. Along with this, the need for secure channels for edge communication is undeniable. Two traits of the quality of desirable network protocols are security and reliability. However, these protocols have associated risks. In this work, we provide an in-depth analysis of dominant network protocols on which the new communication protocols (e.g., CoAP, XMPP, AMQP, etc.) of the Internet of Things (IoT) ecosystem heavily relies on.

Paper ID: 50
Detection of Web Attacks via PART Classifier

Omar Iskndar*, Cihan Varol

University of Duhok, IRAQ
Email: omar94.iskander@gmail.com

***Abstract*—** With the vast and continuous growth in the both computers and communications fields, despite its facilitation of work at all levels, there a number of new challenges the society is facing. The most important of which is the security of sensitive data. With so many hackers wanting to steal sensitive information and exploit it for their own unethical purposes, new protection techniques have to be found. In recent years, Intrusion Detection System (IDS) technology has emerged as an effective option for protecting information within the network. This technology can distinguish between normal traffic and intrusion within the network. In this study, the PART-machine learning classifier algorithm was used to detect web attack attempts based on one of the most recent dataset CICIDS2017. The classifier achieved more than 99% accuracy. RandomForest, NaiveBayes and BayesNet algorithms are also tested for comparison purpose.

Paper ID: 53
A Data Mining Based System for Automating Creation of Cyber Threat Intelligence

Süleyman Muhammed Arıkan*, Sami Acar

*TÜBİTAK BİLGEM, TURKEY
*Email: suleyman.arikan@tubitak.gov.tr

Abstract— In this study, since it is a laborious task to create cyber threat intelligence (CTI), a system that will facilitate the generating of CTI with data mining techniques is proposed. With the system, live or saved traffic records can be classified according to the learned attack types, and CTI can be generated automatically in a standard format. The system is able to update the training set with new attack types by allowing unknown attacks to be identified by expert opinion. The proposed system was designed by a literature survey. Modules of the system have been developed in line with the design, and knowledge discovery in databases processes, including algorithms, have been implemented. In order to verify the achievements of the system, it has been shown that the results of the studies in the literature and the accuracy obtained through the Weka tool, which has proven its reliability in data mining, are similar to the results of the proposed system. Then, the up-to-dateness of the attack types in the preferred dataset was analyzed. As a case study for the application of the proposed system, the traffic was recorded by drawing the attention of the attackers with honeypot systems on a server exposed to the internet for 24 hours, and CTI was generated through these records. It has been shown that the proposed system can be easily used to successfully generate CTI.

Paper ID: 55
Automated Malware Design for Cyber Physical Systems

Ashraf Tantawy*

*Virginia Commonwealth University, USA
*Email: amatantawy@vcu.edu

Abstract— The design of attacks for cyber physical systems is critical to assess CPS resilience at design time and run-time, and to generate rich datasets from testbeds for research. Attacks against cyber physical systems distinguish themselves from IT attacks in that the main objective is to harm the physical system. Therefore, both cyber and physical system knowledge are needed to design such attacks. The current practice to generate attacks either focuses on the cyber part of the system using IT cyber security existing body of knowledge, or uses heuristics to inject attacks that could potentially harm the physical process. In this paper, we present a systematic approach to automatically generate integrity attacks from the CPS safety and control specifications, without knowledge of the physical system or its dynamics. The generated attacks violate the system operational and safety requirements, hence present a genuine test for system resilience. We present an algorithm to automate the malware payload development. Several examples are given throughout the paper to illustrate the proposed approach.

Paper ID: 56
Enterprise Information Systems enhancement: A HyperLedger Fabric based application

Abdelaziz Bouras**,** Houssem Gasmi, **Abdelhak Belhi***, Assam Hammi, Belaid Aouni

*Qatar University, QATAR
Email: abdelhak.belhi@qu.edu.qa

Abstract— Nowadays data analytics and Artificial Intelligence (AI) tools are used at all levels of the extended enterprise, from the shop floor level to run and improve operations, to the strategic process level to make high levels decisions. Failing to provide a unique and fit for all solution, the system providers focus on joining the dots along the digital threads with data continuity in mind. Unfortunately, the existing separate solutions contribute to data overlaps and involve data safety issues. Re-defining the place of the Enterprise Information System components such as Product Lifecycle Management (PLM) and Supply Chain Management (SCM) solutions in a wider digitalization landscape, from product creation to smart factory/Industry 4.0 is the scope of many current works. This includes enhancement in terms of traceability and timely information sharing, addressed through blockchain as digital platforms with features like immutability, transparency, and decentralization of data and information. In this paper, we show how blockchain can overcome such barriers and propose a case study for improving the Enterprise Information System through a blockchain-based solution. The solution would provide more transparent supply chains with improved product traceability as a consequent result of the tamper-proof and decentralization nature of blockchains.

Paper ID: 58
A Comparative Study on the Detection of Image Forgery of Tampered Background or Foreground

Mehmet Elmacı*, Ahmet Nusret Toprak, Veysel Aslantaş

*Erciyes University, TURKEY
*Email: mehmetelmaci@erciyes.edu.tr

Abstract— Recently tampering and manipulating of images has become easier with advanced image editing applications. The process of making a composite image by combining image fragments from different images is called image splicing. One of the common types of image splicing forgery is to change the whole background of the images for different purposes. However, very few studies in the literature directly address the tampered background or foreground detection. We present a comparative study and analysis of image splicing detection methods on the detection of image forgery of tampered background or foreground. First, we create a novel dataset contains both tampered and non-tampered images. Using the dataset, we conduct a comparison of the state-of-the-art image splicing detection methods. The experimental results indicate that existing image splicing detection methods are not sufficient for detecting background or foreground forgeries, and new methods should be developed.

Paper ID: 59
Prevention Pre-Violence in E-Labs with Machine Learning: PVE

Ahmet Furkan Aydoğan*, Narasimha Shashidhar

*Sam Houston State University, USA
*Email: axa184@shsu.edu

Abstract— Digital Forensics continues to be one of the most needed areas of today. In particular, the difficulties experienced in the field of education during the pandemic period have carried the fields where training will be given to the digital parts.However, it also brought pre-pandemic concepts such as bully, violence and insult to cyber environments. Although the studies to improve the existing distance education applications generally focus on areas such as quality image and sound transfer, the ones that may cause bigger problems in the future are the acts called crime. This study aims to create a possible schema to easily complete an investigation that may arise in the future and obtain evidence by applying the Digital Forensics field, which was created to investigate cyber-crime in detail and deliver it to judicial authorities, to distance education applications called elab.In addition, it can be applied to living systems to prevent the aforementioned criminal elements. While the study is performing itself, it focuses on machine learning and natural language processing, and it is seen that it has achieved more than 90% success in small-scale experiments.

Paper ID: 60
A Study of Semiconductor Defects within Automotive Manufacturing using Predictive Analytics

Serkan Varol, **Patrick O'Dougherty***, Keith Ferrel

*University of Tennessee at Chattanooga, USA
*Email: WJG575@mocs.utc.edu

Abstract— Latent defects within semiconductors have been a primary cause of final inspection failures within the electronic control unit (ECU) manufacturing process. Finding the true root
cause within the ECU circuit is a challenge due to the complexity of these devices. As automotive OEMs increase their Tier I testing requirements to eliminate failures within their manufacturing and in the consumer market, Tier I suppliers are reacting by introducing high voltage burn-in testing. The burn-in testing can induce electrical overstress (EOS) to the semiconductors, resulting in requests to Tier II semiconductor manufacturers to analyze these failures. However, the end result is a failure caused within the Tier I process, unrelated to the semiconductor manufacturing process. The analysis of these suspect manufacturers costs both the Tier I and Tier II time and money that could have been used more effectively. Historical data exists within the Tier I manufacturing process that can be analyzed to identify potential relationships between production variables, such as specific equipment used for testing, the temperature of the specific test, the type of measurement taken during that test step, and the result of a non-supplier related defect (NTF or EOS result). A prediction model is created to flag these as potential non-supplier related defects based on previous investigations. The results shift the focus away from the Tier II semiconductor supplier for nonrelated defects and towards solving the root cause which may be occurring within the testing or manufacturing process.

Paper ID: 61
Investigation of Self-Directed Learning Skills of Distance Education Students

Müslim Alanoğlu*, Songül Karabatak, Murat Karabatak

*Tuskish Embassy in Podgorica, MONTENEGRO
*Email: muslimalanoglu@gmail.com

Abstract— During the pandemic, undergraduate students had to motivate, control, and monitor themselves more than students at other education levels. At this point, the importance of selfdirected learning skills that individuals are expected to have has become more evident. For this reason, this research aimed to determine the self-directed learning skill levels of distance undergraduate students and whether these skill levels differ according to the gender variable. For this reason, an easily accessible sampling method was used to reach distance undergraduate students, studying at Firat University in Elazig. The study was conducted with the survey model. Descriptive statistics (kurtosis, skewness values, mean, and standard deviation) were used during the analysis. Independent groups ttest was used to determine whether the students' self-directed learning skills differ according to gender. According to the results, distance undergraduate students always have high selfdirected learning skills, and there is no gender effect on students'self-directed learning skills.

Paper ID: 62
Problems Encountered in Distance Teaching Practices Course and Solution Suggestions

Müslim Alanoğlu*, Songül Karabatak, Murat Karabatak

*Tuskish Embassy in Podgorica, MONTENEGRO
*Email: muslimalanoglu@gmail.com

Abstract— This study aimed to examine the problems experienced by senior students studying at education faculties in the distance Teaching practice (DTP) course, where they participated in practice activities in formal schools due to the Covid-19 pandemic, and the suggestions for solving them. To achieve this aim, the students' opinions, who were determined with purposive sampling in the study conducted with a qualitative research design, were collected with open-ended questionnaires. The results obtained from the study are as follows: (1) The DTP process provided teacher candidates with experience in distance education, increased their technology predispositions, prevented the total interruption of education due to the pandemic, prevented the further spread of the pandemic, and ensured that trainings were conducted independently of time and place. (2) In the DTP process, communication problems between the parties (school administrators, counselors, and students), technical problems, technical impossibilities, inexperience, indifference, and inadequacy of technology use emerged as fundamental problems. (3) For the DTP process to be more effective, teaching practice courses should be fully face-toface, or the DTP process should not only be conducted by distance education but should also be supported by face-to-face education processes.

Paper ID: 63
Review of NLP-based Systems in Digital Forensics and Cybersecurity

David Okore Ukwen*, Murat Karabatak

*National Information Technology, NIGERIA
*Email: ukwendavid@gmail.com

***Abstract*—** Over the years, there is an increase in the use of Artificial Intelligence (AI) by digital forensics and cybersecurity professionals to combat cybercrime. Natural Language Processing (NLP) and AI applications for digital forensics and cybersecurity include data mining, knowledge representation, pattern recognition, and expert systems. This research paper focuses on a literature review of NLP-based systems in digital forensics and cybersecurity: role, applications, challenges, and future directions.This article serves as a guide for researchers and practitioners on the current state of cybersecurity and digital forensics and as well provides a roadmap for the future.

Paper ID: 64
Earthquake Prediction By Using Time Series Analysis

Sultan Lök*, Murat Karabatak

*Fırat University, TURKEY
*Email: loksultan31@gmail.com

Abstract— Nowadays, with the developing technologies, big data stored has started to be formed. Data mining methods have been developed due to the need to obtain information from these stored data. These methods include clustering, classification, association rule, and time series. In this study, time series analysis, one of the data mining methods, was emphasized. Time series provide predictions about future time by time data. Time series are divided into two: linear and non-linear methods. Linear time series methods estimate by assuming that the series is stationary. Non-linear time series methods predict based on the raw version of the series in the real world. In this study, artificial neural networks (ANNs), one of the non-linear methods of Time Series Analysis, are used. Earthquake data were discussed with ANNs. Estimates were made by analyzing earthquake data.

Paper ID: 65
A New Sustainable Hybrid Software Development Methodology: FIRAT-UG

Mustafa Ulaş*, Hakan Güler

*Fırat University, TURKEY
*Email: mustafaulas@firat.edu.tr

Abstract— Software development methods are one of the topics that many researchers have worked on. Methods such as Waterfall, Agile and Scrum are used to develop importantsoftware. All of these proposed methods are for software developers to produce manageable software during software development. However, it is important to ensure the continuity ofhuman resources lossless and sustainable as well as managing software development phases. A new software development method is proposed in this study. With this method, the management of the software development phase will be a model in which human resources are managed integrated by participating in the work. With this model, it is aimed to minimize the potential risks of software development in this sector where is a lack of mobility and scarcity of human resource. The aim is to introduce a new sustainable software development methodology. This model was implemented under the coordination of F.U. Digital Transformation and Software Office and achieved successful results within 2 months. The model has reduced the human resources problems by %66.

Paper ID: 66
Software Engineering for Data Mining (MLEnable) Software Applications

Sabeer Saeed*, Mohammed Mansur Abubakar, Murat Karabatak

*Fırat University, TURKEY
*Email: sabeerawa05@yahoo.com

Abstract— As the data increase keeps on getting more extensive due to technology evolvement from the rational database, online transaction, cloud computing, data warehouse to big data analytics. This changes influences organizations to advance from data mining support to machine learning-enabled software platform. Seemingly, the study summarised secondary data from non-grey and grey academic literature as the research field recently started getting attention. Consequently, the work identifies, analyzes, and synthesizes the challenges of ML-enabled software development, which differs from traditional software development. But, with the adoption of the SE technique to engineer ML-enabled software development, the study was able to identify advancement for ML-enabled software likes automation of mismatch detection, which occurs due to the nature of different perspectives of stakeholders involved. Another one is integrating ML and SE data end-to-end pipeline to allow Systematic test mechanism and test automation where necessary when ML is complex in format to enable standard SE test logs. Then, education, training, and cooperation between the stakeholders, especially SE and ML, to gain more experience, knowledge, put rifts aside to join hands, and work together to ascertain user requirements. Finally, the work reframed the traditional SE development process to engineer the ML software development process. Therefore, the study can benefit stakeholders in the ML and SE communities in handling ML development challenges and may benefits academicians in conduction future research on software engineering for artificial intelligence.

SPONSORS

SOFTWARE AND CYBER SECURITY ASSOCIATION

Elazig – TURKEY

www.softcybersec.org **softcybersec@gmail.com**